Application of Probability Methods in Number Theory and Integral Geometry

Dissertation

zur Erlangung des Doktorgrades

an der Fakultät für Mathematik

der Universität Bielefeld

von Anna Gusakova

October 2018

Gedruckt auf alterungsbeständigem Papier nach DIN ISO-9706.

Abstract

One of the interesting and beautiful aspects of mathematics is the existence of connections between different areas. Such a link is an indication that, using various mathematical notations, one can describe the same event from different points of view. It is not only evidence of the tight relation between numerous mathematical laws, but also a powerful tool which has helped to make progress or good predictions in difficult mathematical problems.

In this thesis we consider a few problems in number theory and integral geometry which both admit a probabilistic interpretation. We solve those problems using methods from probability theory.

In the first part of the thesis we investigate the distribution of algebraic numbers over the field $\mathbb{Q}$, namely we consider the question of counting algebraic numbers and points with algebraic conjugate coordinates in subsets of Euclidean space. Recall that the set of algebraic numbers over the field $\mathbb{Q}$ is the set of roots of polynomials from the polynomial ring $\mathbb{Z}[t]$. There is a natural connection between algebraic numbers and zeroes of random polynomials, which allows us to understand the distribution of algebraic numbers and points with algebraic conjugate coordinates.

We consider several different types of subsets and derive counting formulas or upper and lower estimates for the number of points with algebraic conjugate coordinates lying inside the given subset. We are going to use the following two methods.

- Counting integer points in multidimensional regions and using the connection between algebraic numbers and zeroes of random polynomials.
- The measure-theoretical approach.

We analyze the results obtained by using these methods and describe the limitations that arise when using each of them.

In the second part of the thesis we study questions connected to the distribution of the volume of random simplices, generated as a convex hull of $2 \leq k+1 \leq n+1$ random points $X_0, \ldots, X_k$ in $\mathbb{R}^n$. We interested in how the distribution of the volume of random simplex changes under some fixed affine transformation. Our main result is equality in distribution between the volume of the original simplex and its affine image in terms of determinants of Gaussian random matrices.

Applying the above, we derive a new representation of intrinsic volumes of an ellipsoid and obtain the integral geometry formula connecting the average volume of projections and the average volume of cross-sections of an ellipsoid. Moreover we prove the generalization of integral formula of Furstenberg and Tzkoni [30] and establish its affine version.

Acknowledgments

I would like to express my gratitude to all those people who have supported me while writing this thesis.

I would especially like to thank my adviser Friedrich Götze for his ample advice, motivating discussions and support of my work, Vasili Bernik for introducing me to number theory and setting me on the right path in my research, Dmitry Zaporozhets for presenting a number of interesting problems in integral geometry to me.

I would also like to take this opportunity to thank Ji-Oon Lee who supervised me during my stay in South Korea.

I am grateful to Zakhar Kabluchko, Daniel Hug and Günter Last for fruitful discussions and helpful suggestions.

Finally I would like to thank my family and friends who supported me mentally and helped me to stay positive. I owe my special thanks to Rebecca Reischuk, Nadine Brehme, Anke Bodzin, Claudia Köhler and Anita Lydia Cole for their help during my studies in Bielefeld

The author acknowledges financial support by the German Research Foundation (DFG) through the International Research Training Group *Searching for the regular in the irregular: Analysis of singular and random systems* (IRTG 2235) and Collaborative Research Center *Spectral Structures and Topological Methods in Mathematics* (CRC 701).

Contents

1 Introduction **1**
- 1.1 Notation . . . 1
- 1.2 Distribution of Algebraic Numbers . . . 2
  - 1.2.1 Description of the Problem . . . 2
  - 1.2.2 Results . . . 3
- 1.3 Random Simplices . . . 6
- 1.4 Structure of Thesis . . . 7

2 Counting Complex Algebraic Numbers on the Unit Circle **9**
- 2.1 General Method . . . 9
- 2.2 Connection of the Distribution of Algebraic Numbers and Zeroes of Random Polynomials . . . 12
- 2.3 Main Result . . . 13
- 2.4 Corollaries . . . 15
- 2.5 Proof of Theorem 2.3.2 . . . 16
- 2.6 Proofs of Corollaries . . . 24

3 Counting Points with Algebraic Conjugate Coordinates **31**
- 3.1 Introduction . . . 31
- 3.2 Rectangles of Small Measure . . . 33
  - 3.2.1 Some Technical Lemmas . . . 34
  - 3.2.2 Proof of Theorem 3.2.1: Lower Bound . . . 36
  - 3.2.3 Proof of Theorem 3.2.2: Lower Bound . . . 60
  - 3.2.4 Proof of Theorem 3.2.3: Upper Bound . . . 64
- 3.3 Neighborhood of Curves . . . 65
  - 3.3.1 Main Result . . . 66
  - 3.3.2 Proof: Lower Bound . . . 67
  - 3.3.3 Proof: Upper Bound . . . 69
- 3.4 Distribution of Algebraic Integers and Points with Conjugate Algebraic Integer Coordinates . . . 70
  - 3.4.1 Proof of Theorem 3.4.1 . . . 71
  - 3.4.2 Proof of Theorem 3.4.3 . . . 77

4 Affine Transformation of Random Simplices and Integral Geometry **83**
- 4.1 Main Result . . . 85
  - 4.1.1 Connection with Intrinsic Volumes . . . 86
  - 4.1.2 Connection with Gaussian Random Matrices . . . 86
- 4.2 Random Points in Ellipsoids . . . 87
- 4.3 Integral Geometry Formulas . . . 89
- 4.4 Proofs: Part I . . . 90

4.4.1 Proof of Proposition 4.1.3 . . . 90
4.4.2 Proof of Theorem 4.1.2 . . . 91
4.4.3 Proof of Corollary 4.1.5 . . . 94
4.4.4 Proofs of Theorem 4.2.1 and Theorem 4.2.2 . . . 95
4.4.5 Proof of Corollary 4.2.1.1 . . . 95
4.5 Proofs: Part II . . . 96
4.5.1 Proof of Theorem 4.3.1 . . . 96
4.5.2 Proof of Theorem 4.3.3 . . . 97

A Some Results From Number Theory and Geometry of Numbers 99
A.1 Number Theory . . . 99
A.1.1 Definitions . . . 99
A.1.2 Lemmas . . . 100
A.2 Geometry of Numbers . . . 102

B Random polynomials 105

C Integral Geometry 107
C.1 Intrinsic Volumes . . . 108
C.2 Blaschke-Petkantschin Formulas . . . 109
C.3 Ellipsoids . . . 110

Bibliography 111

Chapter 1

Introduction

This thesis consists of two parts. In the first part we investigate the distribution of algebraic numbers over the field $\mathbb{Q}$, namely we will consider the question of counting algebraic numbers and points with algebraic conjugate coordinates in subsets of Euclidean space. In the second part of the thesis we will study questions connected to the distribution of the volume of random simplices, generated as a convex hull of $2 \leq k+1 \leq n+1$ random points $X_0, \ldots, X_k$ in $\mathbb{R}^n$.

1.1 Notation

Throughout this thesis we will use the following notations and conventions.

- We will denote by:
  - $\#S$ the cardinality of a finite set S;
  - $\lambda_n(S)$ the Lebesgue measure of a measurable set $S \subset \mathbb{R}^n$;
  - $\lambda_L(S)$ the k-dimensional Lebesgue measure on linear or affine k-dimensional subspace $L \subset \mathbb{R}^n$ of a measurable set $S \subset L$;
  - $\mathrm{vol}(D) := \lambda_n(D)$ the n-dimensional volume of a body $D \subset \mathbb{R}^n$;
  - $\mathbb{R}_+$ the set of positive real numbers;
  - $\zeta(\cdot)$ the Riemann zeta function;
  - $\mathbb{B}^n$ the unit n-dimensional ball with volume

$$\kappa_n := \mathrm{vol}(\mathbb{B}^n) = \frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)}.$$

- We will also use the Vinogradov symbol $A \ll B$, which means that there exists a value $c > 0$ such that $A \leq c\,B$ and c does not depend on B. Moreover we will write $A \asymp B$ when $A \ll B$ and $B \ll A$.
- We will also use big O notation $B = O(A)$ which is equivalent to the inequality $|A| \leq c\,B$ for some $c > 0$ independent of B.

1.2 Distribution of Algebraic Numbers

The question of the distribution of real and complex algebraic numbers over the field $\mathbb{Q}$ has been investigating during the last few years and a tight relation between the distribution of algebraic numbers and the distribution of the zeroes of random polynomials has been found. Recall that the number α is called an algebraic number over the field $\mathbb{Q}$ if it is a root of a polynomial $P \in \mathbb{Z}[t]$, irreducible over $\mathbb{Q}$. For the further definitions and properties of algebraic numbers, we refer the reader to Appendix A. In this section we will describe the problem considered in this thesis and make a review of obtained results.

1.2.1 Description of the Problem

Let $\mathbb{A}$ denote the field of algebraic numbers over $\mathbb{Q}$ and $\mathcal{O}$ denote the ring of algebraic integers over $\mathbb{Q}$. Denote by $\mathbb{A}_n$ and $\mathcal{O}_n$ the sets of algebraic numbers and algebraic integers of degree n respectively. Asking about the distribution of algebraic numbers we typically consider the following question. How many algebraic numbers from $\mathbb{A}_n$ or $\mathcal{O}_n$ lie in a given connected set $D \subset \mathbb{C}$? We will assume that $n \geq 2$ since the case $n = 1$ is trivial.

First of all we emphasize that the sets $\mathbb{A}_n$ and $\mathcal{O}_n$ are countable and that any subset D of $\mathbb{R}$ or $\mathbb{C}$ having non-zero measure contains infinitely many algebraic numbers and algebraic integers, even for fixed degree. Thus, in order to study the distribution of algebraic numbers, we need to pick finite subsets of $\mathbb{A}_n$. For this reason we consider a height function $h : \mathbb{A} \to \mathbb{R}_+$, such that for any $n \in \mathbb{N}$ and $Q > 0$ there are only finitely many algebraic numbers $\alpha \in \mathbb{A}_n$ with $h(\alpha) \leq Q$, and $h(\alpha') = h(\alpha)$ for all algebraic conjugates α' and α. This function gives us an order relation on the set $\mathbb{A}_n$. In this thesis we will consider two types of height function, namely the 'naïve' height and the elliptic height, which is a special case of the weighted l_p height.

Given some algebraic number α denote by $P_\alpha(t) = a_n t^n + \ldots + a_1 t + a_0$ its minimal polynomial.

The *'naïve' height* H of an algebraic number α is equal to the 'naïve' height of its minimal polynomial P_α which is defined as follows

$$H(\alpha) = H(P_\alpha) := \max_{0 \leq i \leq n} |a_i|.$$

This type of height function is very natural and may be considered as a measure of 'algebraic complexity' needed to describe the element.

The weighted l_p-height is not so often used. It can be viewed as a generalization of the 'naïve' height. Given a vector of positive weights $\mathbf{w} = (w_0, w_1, \ldots, w_n) \in \mathbb{R}_+^{n+1}$ and a real number $0 < p \leq \infty$ define the $\mathbf{w}$-weighted l_p height of an algebraic

number α as follows

$$l_{p,\mathbf{w}}(\alpha) := \begin{cases} \left(\sum\limits_{i=0}^{n} |w_i\, a_i|^p \right)^{1/p}, & p < \infty; \\ \max\limits_{0 \le i \le n} \left(w_i\, |a_i| \right), & p = \infty. \end{cases}$$

For any vector of weights we will say that the function $h_{\mathbf{w}} := l_{2,\mathbf{w}}$ is the *elliptic height* of an algebraic number α.

Finally, let $\mathbb{A}_n(Q)$ be the set of algebraic numbers $\alpha \in \mathbb{A}_n$ with $H(\alpha) \le Q$ and let $\mathcal{O}_n(Q)$ be the set of algebraic integers $\alpha \in \mathcal{O}_n$ with $H(\alpha) \le Q$. Moreover, denote by $\mathbb{A}_{n,\mathbf{w}}(Q)$ the set of algebraic numbers α of degree n with $h_{\mathbf{w}}(\alpha) \le Q$.

1.2.2 Results

Distribution of Complex Algebraic Numbers on the Unit Circle .

Consider the unit circle $\mathbb{T} \subset \mathbb{C}$ and for $-\pi \le \beta_1 < \beta_2 \le \pi$ denote by

$$\mathbb{T}_{\beta_1,\beta_2} := \{z \in \mathbb{T} \colon \operatorname{Arg}(z) \in [\beta_1, \beta_2]\},$$

some arc of the circle $\mathbb{T}$.

The first result of the thesis is the asymptotic formula for the number of complex algebraic numbers of degree n and elliptic height at most Q lying on a given arc $\mathbb{T}_{\beta_1,\beta_2}$

$$\mathcal{N}_{n,\mathbf{w}}(Q, \beta_1, \beta_2) := \#\left(\mathbb{A}_{n,\mathbf{w}}(Q) \cap \mathbb{T}_{\beta_1,\beta_2}\right)$$

as $Q \to \infty$.

For any even $n = 2m \ge 2$, any $-\pi \le \beta_1 < \beta_2 \le \pi$, and any vector of positive weights $\mathbf{w} \in \mathbb{R}_+^{2m+1}$ with $w_i = w_{2m-i}$ for all $0 \le i \le 2m$ we obtain

$$\mathcal{N}_{2m,\mathbf{w}}(Q, \beta_1, \beta_2) = v(m, \mathbf{w})\, Q^{m+1} \int\limits_{\beta_1}^{\beta_2} p_{\mathbf{w},m}(t)\, dt + O\left(Q^m\, (\log Q)^{\lfloor 2/m \rfloor} \right), \quad (1.2.1)$$

where

$$v(m, \mathbf{w}) := \frac{\operatorname{vol}(\mathbb{B}^{m+1})}{2^{m/2+1} \zeta(m+1) w_0 \dots w_m},$$

and the function $p_{\mathbf{w},m}(t)$ is given explicitly below. Moreover, for odd n we show that $\mathcal{N}_{n,\mathbf{w}}(Q, \beta_1, \beta_2) = 0$ for any $\mathbf{w} \in \mathbb{R}_+^{2m+1}$ and $-\pi \le \beta_1 < \beta_2 \le \pi$. It should be also noted that our method works for any weighted l_p-norm (including the 'naïve' height), but we consider the elliptic height only, since this case admits the simplest type of asymptotic distribution formula.

In order to derive formula (1.2.1) we apply a method based on counting lattice points in domains of Euclidean space. The description of the method can be found

in Section 2.1. Using this method we show that the function $p_{\mathbf{w},m}(t)$ is equal to the density function $\rho_{m,T}(t)$ of the zeroes of the random trigonometric polynomial

$$T(\theta) := \frac{\eta_m}{2\,w_m} + \sum_{k=1}^{m} \frac{\eta_{m-k}}{\sqrt{2}\,w_{m-k}} \cos k\theta,$$

where $\eta_0, \dots, \eta_m$ are independent, identically distributed real-valued standard Gaussian random variables. This fact is evidence of a tight relation between the distribution of algebraic numbers and the distributions of zeroes of random polynomials. More examples of such relations are given in Section 2.2. For the precise definition of a density function and discussion of the distribution of zeroes of random polynomials see Appendix B.

In general it is a very difficult task to derive the exact formulas for the density functions of zeroes of random trigonometric polynomials with arbitrary distribution of coefficients. Although, if we restrict our attention to the case where the coefficients are Gaussian random variables, the function $\rho_{m,T}(t)$ can be computed in a precise form, using the Kac-Rice formula and special properties of Gaussian random variables. For example, it follows from the result of Edelman and Kostlan [26] that

$$\rho_{n,T}(t) = \frac{1}{\pi} \left[\frac{\partial^2}{\partial x \partial y} \log \left(\frac{w_m^{-2}}{2} + \sum_{k=1}^{m} w_{m-k}^{-2} \cos(kx) \cos(ky) \right) \Big|_{x=y=t} \right]^{1/2},$$

which gives us the representation for the function $p_{\mathbf{w},m}(t)$ in formula (1.2.1).

The result (1.2.1) is obtained in joint work with Friedrich Götze, Zakhar Kabluchko, and Dmitry Zaporozhets [33]. For a more detailed discussion of the problem, see Chapter 2.

Distribution of Points with Algebraic Conjugate Coordinates .

The next result of the thesis describes the two-dimensional problem where, instead of algebraic numbers, we consider points with algebraic conjugate coordinates. Given a Borel subset $D \subset \mathbb{R}^2$, consider the function $\mathcal{N}_n^2(\mathbb{A}, Q, D)$, which counts the number of ordered pairs $\boldsymbol{\alpha} := (\alpha_1, \alpha_2)$ of distinct conjugate algebraic numbers α_1, α_2 of degree at most n and 'naïve' height at most Q lying within a subset D.

In case of fixed subset $D \in \mathbb{R}^2$ the asymptotic formula for $\mathcal{N}_n^2(\mathbb{A}, Q, D)$ follows from a more general result of Kaliada, Zaporozhets, and Götze [35]. In this thesis we consider subsets with fixed 'position' and measure depending on Q that vanishes as Q tends to infinity.

The first class of subsets under consideration are rectangles $\Pi = I_1 \times I_2$ with fixed middle point and sizes $\lambda_1(I_1) \asymp Q^{-s_1}$, $\lambda_1(I_2) \asymp Q^{-s_2}$, where $s_1, s_2 > 0$. Under some additional conditions on values s_1 and s_2 we derive the following upper and lower bounds for the value $\mathcal{N}_n^2(\mathbb{A}, Q, \Pi)$, which are asymptotically the same as Q tends to infinity

$$\mathcal{N}_n^2(\mathbb{A}, Q, \Pi) \asymp Q^{n+1} \lambda_2(\Pi). \tag{1.2.2}$$

For the more details we refer reader to Section 3.2.

The second class are some ϵ-neighborhoods of a fixed curve defined by a function f, where $\epsilon \asymp Q^{-\lambda}$, $\lambda > 0$. In should be noted that the problem of counting points with rational coordinates in the neighborhood of curves has a rich history [41, 64, 8] and the problem of counting points with algebraic conjugate coordinates near the curves may be regarded as its generalization. Considering the set

$$L^f_{\lambda,J} := \left\{ \mathbf{x} \in \mathbb{R}^2 \colon |x_2 - f(x_1)| < C_1\, Q^{-\lambda}, \quad x_1 \in J \right\},$$

we obtain the following asymptotic estimates as Q tends to infinity

$$\mathcal{N}^2_n \left(\mathbb{A}, Q, L^f_{\lambda,J} \right) \asymp Q^{n+1-\lambda}, \tag{1.2.3}$$

where $0 < \lambda < \frac{3}{4}$ and function f satisfies some additional smoothness conditions. See Section 3.3 for the precise statement and a historical review.

The results above are based on joint work with Friedrich Götze, and Vasili Bernik [12].

Distribution of Algebraic Integers .

The last result of this section is connected with the distribution of algebraic integers. In contrast to algebraic numbers, algebraic integers are usually more difficult to analyze. In particular, powerful tools like the method of counting lattice points does not yield any good results here.

Given an interval $I \subset \mathbb{R}$, let us denote by

$$\mathcal{N}_n(\mathcal{O}, Q, I) := \#\left(\mathcal{O}_n(Q) \cap I\right)$$

the number of algebraic integers α of degree n and 'naïve' height at most Q belonging to the interval I.

We show that for any interval I of length $\lambda_1(I) \asymp Q^{-s}$, $0 < s \leq 1$ with fixed middle point the following asymptotic bounds

$$\mathcal{N}_n\left(\mathcal{O}, Q, I\right) \asymp Q^n\, \lambda_1\left(I\right), \tag{1.2.4}$$

hold as Q tends to infinity.

We also consider the two-dimensional problem analogous to the one formulated for points with algebraic conjugate coordinates. Given a Borel subset $D \subset \mathbb{R}^2$, consider the function $\mathcal{N}^2_n(\mathcal{O}, Q, D)$, which counts the number of ordered pairs $\boldsymbol{\alpha} := (\alpha_1, \alpha_2)$ of distinct conjugate algebraic integers α_1, α_2 of degree n and 'naïve' height at most Q lying within a subset D.

For the rectangles $\Pi = I_1 \times I_2$ with fixed middle point and sizes $\lambda_1(I_1) \asymp Q^{-s_1}$, $\lambda_1(I_2) \asymp Q^{-s_2}$ we derive the following asymptotic estimates

$$\mathcal{N}^2_n\left(\mathcal{O}, Q, \Pi\right) \asymp Q^n \lambda_2\left(\Pi\right), \tag{1.2.5}$$

and for the ϵ-neighborhood of some fixed curve defined by the function f with $\epsilon \asymp Q^{-\lambda}$ we obtain

$$\mathcal{N}_n^2\left(\mathcal{O}, Q, L^f_{\lambda,J}\right) \asymp Q^{n-\lambda}, \tag{1.2.6}$$

as Q tends to infinity.

These formulas are based on joint work with Friedrich Götze [32]. The detailed description can be found in Subsection 3.4.

1.3 Random Simplices

The study of geometric probability is concerned with randomly generated geometric objects (points, lines, convex bodies, etc.) and simple operations with them (taking convex or linear hull, considering intersection, etc.), as well as random transformations (rotation, projection on random hyperplane, etc.). The assignment of a probability measure to geometric objects and transformations is not necessarily an obvious procedure and can lead to ambiguity. Therefore, one should specify how the random geometric object is generated. Many questions of geometric probability are easy to formulate, but usually very difficult to answer. The important point is that geometric probability and integral geometry are closely related and some problems of geometric probability can be easier solved with the help of the integral geometry methods and vice versa. In this thesis we consider a special class of random geometric objects, namely the convex hull of randomly generated points in $\mathbb{R}^n$.

Consider $k+1$ random points $X_0, \dots, X_k$ in $\mathbb{R}^n$. Denote by

$$\operatorname{conv}(X_0, \dots, X_k)$$

the convex hull of points $X_0, \dots, X_k$, which is the the smallest convex set that contains all of them. This convex hull is an example of random polytope with vertices $X_0, \dots, X_k$. If $1 \le k \le n$ then the random polytope $\operatorname{conv}(X_0, \dots, X_k)$ is a k-dimensional simplex (maybe degenerate). Denote by

$$\Delta_k\left(X_0, \dots, X_k\right) := \operatorname{vol}\left(\operatorname{conv}(X_0, \dots, X_k)\right) \tag{1.3.1}$$

the k-dimensional volume of the simplex $\operatorname{conv}(X_0, \dots, X_k)$.

In this thesis we investigate how the distribution of (1.3.1) changes under some fixed affine transformation $\mathbf{x} \to A\mathbf{x}$, where A is a non-singular $n \times n$ matrix. We derive the following stochastic equation

$$\Delta_k(AX_0, \dots, AX_k) \stackrel{d}{=} \frac{\operatorname{vol}\left(P_\xi \mathcal{E}\right)}{\kappa_k} \cdot \Delta_k(X_0, \dots, X_k), \tag{1.3.2}$$

where the random vectors $X_0, \dots, X_k$ are not necessary independent, identically distributed and have an arbitrary *spherically symmetric* joint distribution, $\mathcal{E}$ is the ellipsoid defined as the image of the unit ball $\mathbb{B}^n$ under an affine transformation $A^\top$, κ_k is the volume of the k-dimensional unit ball $\mathbb{B}^k$, P_L denotes the orthogonal

projection operator on the linear subspace $L \subset \mathbb{R}^n$, and ξ is a random uniformly chosen k-dimensional linear subspace, independent of $X_0, \dots, X_k$.

Due to the spherical symmetry of the joint distribution of $X_0, \dots, X_k$ we can obtain a probabilistic representation of the random value $\mathrm{vol}\,(P_\xi \mathcal{E})$ in terms of determinants of the Gaussian random matrices

$$\frac{\mathrm{vol}(P_\xi \mathcal{E})}{\kappa_k} \stackrel{d}{=} \left(\frac{\det\left(G^\top A^\top A G\right)}{\det\left(G^\top G\right)} \right)^{1/2}, \tag{1.3.3}$$

where G is a random $n \times k$ matrix with independent, identically distributed standard Gaussian entries.

The result above leads to some interesting integral geometry formulas. For a detailed discussion we refer the reader to Chapter 4.

The results of this section are based on joint work with Friedrich Götze and Dmitry Zaporozhets [34].

1.4 Structure of Thesis

The structure of this thesis is the following. In Chapter 2, we prove formula (1.2.1) and calculate the function $p_{\mathbf{w},n}(t)$ for some vectors $\mathbf{w}$. In Chapter 3, we discuss the results formulated in (1.2.2) — (1.2.6). In Chapter 4 we prove the main results (1.3.2) and (1.3.3) and consider the applications to integral geometry problems. All auxiliary results and necessary definitions are presented in Appendices A — C.

Chapter 2

Counting Complex Algebraic Numbers on the Unit Circle

In this chapter, we study the distribution of algebraic numbers on the unit circle in the complex plane which we denote by $\mathbb{T} \subset \mathbb{C}$. For $-\pi \leq \beta_1 < \beta_2 \leq \pi$ denote by

$$\mathbb{T}_{\beta_1,\beta_2} := \{z \in \mathbb{T} \colon \operatorname{Arg}(z) \in [\beta_1, \beta_2]\}$$

some arc of the unit circle $\mathbb{T}$. Our goal is to investigate the asymptotic behavior of the value

$$\mathcal{N}_{n,\mathbf{w}}(Q, \beta_1, \beta_2) := \#\left\{\theta \in [\beta_1, \beta_2] \colon e^{i\theta} \in \mathbb{A}_{n,\mathbf{w}}(Q)\right\},$$

which is equal to number of complex algebraic numbers of degree n and elliptic height at most Q lying on the arc $\mathbb{T}_{\beta_1,\beta_2}$.

We start with description of the general method used in the proof of our main theorem and make a brief review of previous results and their connection to random polynomials.

2.1 General Method

The easiest way to count algebraic numbers over $\mathbb{Q}$ is to count the corresponding minimal polynomials with integer coefficients instead. The minimal polynomial P_α of a given algebraic number α of degree n is uniquely defined, irreducible, has co-prime coefficients, and has exactly n roots. Thus, the conditions on α typically lead to analogous restrictions for the coefficients $a_n, \ldots, a_0$ of the polynomial P_α, and the problem of counting algebraic numbers α of degree n satisfying certain conditions is analogous to counting irreducible polynomials of degree n with co-prime integer coefficients under some restrictions.

Assuming next that those restrictions define the bounded set $V \subset \mathbb{R}^{n+1}$ and identifying the polynomial P with its vector of coefficients $(a_n, \ldots, a_0) \in \mathbb{Z}^{n+1}$ we reduce the original problem of counting algebraic numbers to the counting of lattice points in the set V. The last problem is well known and a lot of good estimates have been obtained.

Two additional steps are needed in order to exclude from the consideration points $(a_n, \ldots, a_0) \in \mathbb{Z}^{n+1}$ with $\gcd(a_n, \ldots, a_0) > 1$ and points $(a_n, \ldots, a_0) \in \mathbb{Z}^{n+1}$ which

define a reducible polynomial $P(t) = a_n t^n + \ldots + a_0$. The first step can be easily realized using the classical Möbius inversion formula (see, e.g., [55]). The second step is the counting of reducible polynomials which is an old problem in number theory.

2.1.0.1 Counting Lattice Points

The problem of counting lattice point in a given bounded subset of $\mathbb{R}^n$ is an important topic in geometry of numbers and goes back to the old results by Lipschitz (1865) and Davenport (1964). Consider some bounded set $D \subset \mathbb{R}^n$ and some lattice $\Lambda \subset \mathbb{R}^n$. The basic idea says that in case the set D possess some 'nice' boundary properties the number of lattice points in D is approximately equal to the volume of the set D divided by the determinant of the lattice Λ. The main difficulty is to check this property and to estimate the error term

$$r(D, \Lambda) = \left| \mu_\Lambda(D) - \frac{\mathrm{vol}(D)}{\det(\Lambda)} \right|,$$

where $\mu_\Lambda(D)$ denotes the number of lattice points in D. There is an extensive literature on this topic and here we consider two classes of sets D, outlined below.

1. The first and the oldest class of sets was introduced by Lipschitz [48]. He considered the sets D with boundary ∂D which can be defined by finitely many maps $\phi_1, \ldots, \phi_M : [0,1]^{n-1} \to \mathbb{R}^n$ satisfying Lipschitz condition with some constant L. We say that the boundary ∂D is of Lipschitz class (n, M, L). Later on the results of Lipschits were extended in [61] and [46, Chapter VI, §2, Theorem 2]. In these papers only the homogeneously expanding sets were considered, namely the sets of type

   $$tD = \{t\mathbf{x} : \mathbf{x} \in D\},$$

   where D is some fixed bounded set and $t \in \mathbb{R}_+$ is assumed to be some growing parameter. The error term in this case has the form $r(tD, \Lambda) = O(t^{n-1})$, where the implicit constant depends on Λ, n, M and L only. The counting result for an arbitrary bounded sets D with boundary ∂D of Lipschitz class (n, M, L) was obtained by Masser and Vaaler [49]. They also proved an estimate for the error term $r(D, \Lambda)$ in terms of the parameters n, M, L and the successive minima of the lattice Λ. Similar results with a sharp error term were obtained by Widmer [66].

2. Another class of sets was firstly defined by Davenport [22]. His approach is applicable to bounded measurable sets D which intersect every line in at most s intervals or single points and the same is required for any projection of D on any linear subspace of $\mathbb{R}^n$. We say that such sets are of narrow class s, in accordance with [67]. Davenport considered the case $\Lambda = \mathbb{Z}^n$ only and derived an estimate for $r(D, \Lambda)$ in terms of the measures of all projections of the set D on linear subspaces of $\mathbb{R}^n$. This result was further generalized by Schmidt

in [58], where he obtained a counting result for an arbitrary lattice and gave an estimate for the error term in terms of the diameter of the set D and the successive minima of the lattice Λ. The next improvement was made in [3], where the best possible estimate for the error term was obtained.

Let us stress that for both classes of sets introduced above we get the same counting result. Therefore it is very natural to ask for relationships between these classes and whether one class includes the other. This question was addressed in the article of Masser and Vaaler [49] where they pointed out that the sets with Lipschitz boundary do not necessary belong to the narrow class, but narrow class possibly implies some type of sets with Lipschitz boundary. A more careful analysis is due to Widmer [67]. In particular, Widmer has described the case where the bounded set of narrow class 1 has a boundary of a Lipschitz class (see Theorem A.2.9). It should be noted that in general it is not an easy task to verify that some given set D is of narrow class or has a Lipschitz parameterizable boundary.

Although there are general results with better estimates of the error $r(D, \Lambda)$, we shall use the result of Lang [46, Chapter VI, §2, Theorem 2] for homogeneously expanding sets (see Theorem A.2.7) since it will be enough for our case.

2.1.0.2 Counting Reducible Polynomials

An important and difficult problem in general is to determine whether a given polynomial $P \in \mathbb{Z}[t]$ is irreducible over $\mathbb{Q}$ or not. There exist a few results which give sufficient conditions for a polynomial to be irreducible, such as Eisenstein's criterion (see Lemma A.1.20) and Cohn's irreducibility criterion for example. Unfortunately, they are quite far from being useful, since they cover only a small part of the set of all irreducible polynomials [24]. The problem of finding a general criterion of irreducibility for polynomials is very difficult and probably remains open.

On the other hand it is easier to prove that the majority of polynomials is irreducible. In order to do so we will construct the finite subsets of polynomials $P \in \mathbb{Z}[t]$, considering only polynomials with bounded 'naïve' height. Denote by $\mathcal{R}_H(n, Q)$ the number of reducible polynomials $P \in \mathbb{Z}[t]$ of degree n and $H(P) \leq Q$.

The first step was made by van der Waerden [65] in 1934 who proved that almost all polynomials $P \in \mathbb{Z}[t]$ are irreducible over the $\mathbb{Q}$. He considered the subset of polynomials $P \in \mathbb{Z}[t]$ of degree n and $H(P) \leq Q$ and proved that only a small part of them can be factorized into product of two integer polynomials of given degrees. On the other hand this result does not give any precise information about the value $\mathcal{R}_H(n, Q)$. The true order of $\mathcal{R}_H(n, Q)$ was recently found by Kuba [45]. He showed that $\mathcal{R}_H(n, Q) \asymp Q^n (\log Q)^{\lfloor 2/n \rfloor}$, $n \geq 2$ as $Q \to \infty$. It should be noted that this result holds for the set of polynomials of degree *at most* n but with different constants. The exact asymptotic for $\mathcal{R}_H(n, Q)$ was given by Dubickas [25].

2.2 Connection of the Distribution of Algebraic Numbers and Zeroes of Random Polynomials

In this subsection we will give a review of the previous results providing an asymptotic formula for the number of points with algebraic conjugate coordinates lying in a given subset D. These results are based on applying the method described above and using the connection between algebraic numbers and zeroes of random polynomials.

Let us formulate the general problem. Given some fixed integer numbers $k, l \geq 0$ such that $0 < k + 2l \leq n$, a Borel subset $D \subset \mathbb{R}^k \times \mathbb{C}_+^l$, a height function h and a positive real number $Q \in \mathbb{R}_+$, consider the function $\mathcal{N}_n^{(k,l)}(Q, D)$ which counts the number of ordered mixed (k,l)-tuples $\boldsymbol{\alpha} := (\alpha_1, \alpha_2, \ldots, \alpha_{k+l})$ of distinct conjugate algebraic numbers α_i of degree at most n and with $h(\alpha_i) \leq Q$, lying within the subset D. Let us emphasize that we assume that $\alpha_1, \ldots, \alpha_k$ are real algebraic numbers and $\alpha_{k+1}, \ldots, \alpha_{k+l}$ are totally complex algebraic numbers. Moreover, since we are considering algebraic numbers over the field $\mathbb{Q}$, the set of algebraic conjugate numbers is invariant under complex conjugation. This means that we can confine ourselves to considering only the upper complex half-plane $\mathbb{C}_+$. Thus, the question regarding the distribution of algebraic numbers reads as follows. Given some fixed integer numbers $k, l \geq 0$ such that $0 < k+2l \leq n$, a Borel subset $D \subset \mathbb{R}^k \times \mathbb{C}_+^l$ and a height function h we need to find the asymptotic behavior of the value $\mathcal{N}_n^{(k,l)}(Q, D)$ as $Q \to \infty$.

The first result in this direction has been obtained by Kaliada [44]. He considered the case of an interval $I \subset \mathbb{R}$ and 'naïve' height $h = H$, and proved the following formula

$$\mathcal{N}_n^{(1,0)}(Q, I) = \frac{Q^{n+1}}{2\zeta(n+1)} \int\limits_I \rho_n^{(1,0)}(x)\, dx + O\left(Q^n (\log Q)^{\lfloor 2/n \rfloor}\right),$$

where the function $\rho_n^{(1,0)} : \mathbb{R} \to \mathbb{R}$ is given explicitly but has a difficult structure. The main problem here was to calculate the volume of the body A_l formed by polynomials with real coefficients, of degree at most n, 'naïve' height at most 1 and having exactly $1 \leq l \leq n$ roots in the interval I. Using some detailed analysis and arguments from number theory Kaliada showed that

$$\sum_{l=1}^{n} l \ \mathrm{vol}(A_l) = \int\limits_I \rho_n^{(1,0)}(x)\, dx, \tag{2.2.1}$$

from which the formula above follows immediately.

Looking carefully at equation (2.2.1) one realizes that the sum in the left side is (up to constant) equal to the expected value of the number of zeroes of the random polynomial $G(t) = \xi_n t^n + \ldots + \xi_1 t + \xi_0$ lying inside the interval I, where the coefficients ξ_i are independent random variables uniformly distributed in the interval

$[-1;1]$. The function $\rho_n^{(1,0)}$ is called the density function of the number of real zeroes of the random polynomial G.

Based on this observation, Kaliada, Zaporozhets, and Götze [36, 35, 37] obtained asymptotic formulas of the same type for more general cases. The key step of their proofs was to derive a formula for the mixed (k,l)-correlation function $\rho_{n,G}^{(k,l)}$ of zeroes of random polynomial G (see the Definition B.0.2). We will mention here the last and most general result only.

For any $p \in (0,\infty]$ and any fixed vector $\mathbf{w} \in \mathbb{R}_+^{n+1}$ consider weighted l_p-height $h = l_{p,\mathbf{w}}$. Then for some integers $k, l \geq 0$, such that $0 < k + 2l \leq n$, and any measurable set $D \subset \mathbb{R}^k \times \mathbb{C}_+^l$, such that its boundary belongs to Lipschitz class $\mathrm{Lip}(n, M, L)$ (see the Definition A.2.6), we have

$$\mathcal{N}_n^{(k,l)}(Q, D) = \frac{\mathrm{vol}(\mathbb{B}_p^{n+1})Q^{n+1}}{2\zeta(n+1)w_0 \dots w_n} \int\limits_D \rho_{n,G}^{(k,l)}(\mathbf{x}, \mathbf{z})\, d\mathbf{x}\, d\mathbf{z} + O\left(Q^n (\log Q)^{\lfloor 2/(n-2l)\rfloor}\right), \quad (2.2.2)$$

where $\mathbb{B}_p^n$ denotes the unit n-dimensional l_p-ball and $\rho_{n,G}^{(k,l)}$ is the mixed (k,l)-correlation function of zeroes of random polynomial $G(z) := \sum\limits_{i=0}^{n} w_i^{-1}\xi_i z^i$, where ξ_i are independent, identically distributed real random variables with a probability density function given by

$$f(t) := \begin{cases} \frac{e^{-|t|^p}}{2\Gamma\left(1+\frac{1}{p}\right)}, & p < \infty, \\ \frac{1}{2}\mathbb{1}_{[-1;1]}(t), & p = \infty. \end{cases}$$

The exact formula for the function $\rho_{n,G}^{(k,l)}$ was also derived in [37].

2.3 Main Result

In this section we formulate our main result.

Let $\mathcal{P}_{n,\mathbf{w}}(Q)$ denote the class of integer polynomials of degree n and with elliptic height at most Q

$$\mathcal{P}_{n,\mathbf{w}}(Q) := \{P \in \mathbb{Z}[t] \colon \deg P = n,\, h_{\mathbf{w}}(P) \leq Q\}.$$

We say that an integer polynomial is *prime*, if it is irreducible over $\mathbb{Q}$, primitive and its leading coefficient is positive. Denote by $\mathcal{P}_{n,\mathbf{w}}^*(Q)$ the class of prime polynomials from $\mathcal{P}_{n,\mathbf{w}}(Q)$

$$\mathcal{P}_{n,\mathbf{w}}^*(Q) := \{P \in \mathcal{P}_{n,\mathbf{w}}(Q) \colon P \text{ is prime},\},$$

which is obviously coincide with the set of minimal polynomials of the set of algebraic numbers of degree n and with elliptic height at most Q.

Let us start with proving an easy fact about the algebraic numbers on the unit circle.

Proposition 2.3.1. *Any algebraic number on $\mathbb{T}$, except for ± 1, has even degree and its minimal polynomial is reciprocal.*

Proof. Consider an algebraic number $\alpha \in \mathbb{T}$ with minimal polynomial

$$P_\alpha(t) = a_n t^n + \ldots + a_1 t + a_0.$$

Since the coefficients of P are real, the complex conjugate $\bar{\alpha}$ is also a root of P. Moreover, $\alpha \in \mathbb{T}$ is equivalent to $|\alpha| = 1$ and, hence, $\bar{\alpha} = \alpha^{-1}$. Thus,

$$P_\alpha(\alpha) = P_\alpha\left(\frac{1}{\alpha}\right) = 0,$$

which implies that α is a root of the polynomial

$$\tilde{P}_\alpha(t) = t^n P_\alpha(t^{-1}) = a_0 t^n + \ldots + a_{n-1} t + a_n.$$

According to the definition of minimal polynomial we conclude that P_α is a factor of $\tilde{P}_\alpha$ and, moreover, there are only two possibilities: $P_\alpha \equiv -\tilde{P}_\alpha$ or $P_\alpha \equiv \tilde{P}_\alpha$. The first would imply that 1 is a root of polynomial P_α which is impossible due to its irreducibility. Therefore $P_\alpha \equiv \tilde{P}_\alpha$ which means that polynomial P_α is reciprocal and

$$a_i = a_{n-i}, \quad 0 \le i \le n.$$

For odd n, this condition implies that -1 is a root of P which, again, contradicts with its irreducibility. □

From the Proposition 2.3.1 we immediately conclude the following.

Corollary 2.3.1.1. *For any fixed vector of positive weights $\mathbf{w}$, any $-\pi \le \beta_1 < \beta_2 \le \pi$ and odd $n \ge 3$ we have*

$$\mathcal{N}_{n,\mathbf{w}}(Q, \beta_1, \beta_2) = 0.$$

Thus, from now on we can restrict our attention to the even n. In this case we prove the following theorem, which is the main result of this chapter.

Theorem 2.3.2. *For any integer even $n = 2m$, $m \ge 1$, any fixed symmetric vector of positive weights $\mathbf{w} = (w_0, \ldots, w_m, \ldots, w_0)$, and any $-\pi \le \beta_1 < \beta_2 \le \pi$ we have*

$$\mathcal{N}_{2m,\mathbf{w}}(Q, \beta_1, \beta_2) = \frac{\mathrm{vol}(\mathbb{B}^{m+1}) Q^{m+1}}{2^{m/2+1} \zeta(m+1) w_0 \ldots w_m} \int_{\beta_1}^{\beta_2} p_{\mathbf{w},m}(t)\, dt + O\left(Q^m (\log Q)^{\lfloor 2/m \rfloor}\right),$$

as $Q \to \infty$, where $\zeta(\cdot)$ denotes the Riemann zeta function and the function $p_{\mathbf{w},m}(t)$ has the form

$$p_{\mathbf{w},m}(t) = \frac{1}{\pi}\left[\frac{\partial^2}{\partial x \partial y} \log\left(\frac{w_m^{-2}}{2} + \sum_{k=1}^{m} w_{m-k}^{-2} \cos(kx)\cos(ky)\right)\Big|_{x=y=t}\right]^{1/2}. \quad (2.3.1)$$

2.4 Corollaries

It should be noted that in general form the limit density $p_{\mathbf{w},m}$ is difficult to analyze. However, for some special vectors $\mathbf{w}$ the expression (2.3.1) can be simplified.

The first one is the Bombieri 2-norm.

Corollary 2.4.0.1. *For any integer $m \geq 1$ and $\mathbf{w} = \left(\binom{2m}{k}^{-1/2}\right)_{k=0}^{2m}$ we have*

$$p_{\mathbf{w},m}(t) = \sqrt{\frac{m}{2\pi^2}} \cdot \frac{|\sin t| \left(\sum_{k=0}^{2m-2} (\cos t)^{2k} + (2m-1)(\cos t)^{2m-2}\right)^{1/2}}{(\cos t)^{2m} + 1}.$$

Let us mention that the Bombieri 2-norm is quite 'natural' to be considered in this case. Particularly for the random polynomial

$$G(z) = \sum_{i=0}^{n} \binom{n}{k}^{1/2} \xi_k z^k$$

with coefficients ξ_k being i.i.d standard Gaussian random variables, the density function of zeroes has a very simple form, see [26], and is given by

$$\rho_{n,G}^{(1,0)}(t) = \frac{\sqrt{n}}{\pi(1+t^2)},$$

which coincides with the normalized Cauchy density.

The next example is the Euclidean height, namely the vector $\mathbf{w} = (1, \ldots, 1)$.

Corollary 2.4.0.2. *For any integer $m \geq 1$ and $\mathbf{w} = (1, \ldots, 1)$ we have*

$$p_{\mathbf{w},m}(t) = \frac{1}{\pi}\left(b_m + \frac{\sin(b_m t)}{\sin t}\right)^{-1} \cdot \Big(\frac{b_m \sin(b_m t)}{2(\sin t)^3} - \frac{b_m^2}{2}\frac{\cos(b_m t)\cos t}{(\sin t)^2} + \frac{(\sin(b_m t))^2}{4(\sin t)^4} - \frac{b_m^3 + 2b_m}{6}\frac{\sin(b_m t)}{\sin t} - \frac{b_m^2}{4(\sin t)^2} + \frac{(m^2+m)b_m^2}{3}\Big)^{1/2},$$

where $b_m = 2m + 1$.

The last example is very specific family of weight vectors depending on some positive parameter a.

Corollary 2.4.0.3. *Consider the vector of weights $\mathbf{w} \in \mathbb{R}_+^{2m}$ for $m = 2k$ defined as*

$$\begin{cases} w_{2(k-j)-1} = \left(4^{-k}\sum_{i=1}^{k-j}\binom{2k}{2i-1}\binom{2k-2i+1}{k-i-j}(2a)^{2i-1}\right)^{-1/2}, & 0 \leq j \leq k-1; \\ w_{2(k-j)} = \left(4^{-k+1}\sum_{i=0}^{k-j}\binom{2k}{2i}\binom{2k-2i}{k-i-j}(2a)^{2i}\right)^{-1/2}, & 0 \leq j \leq k; \end{cases} \tag{2.4.1}$$

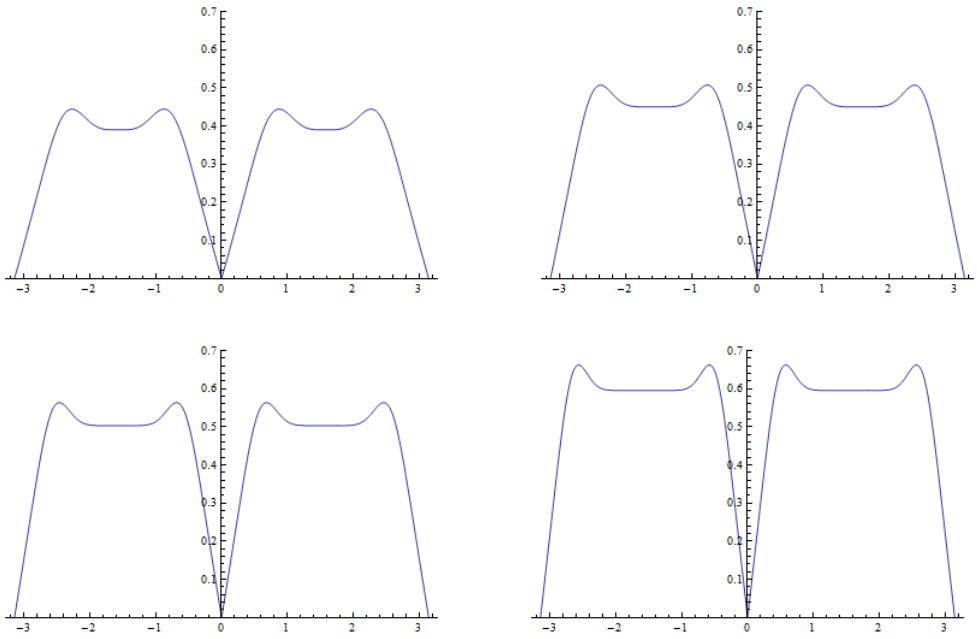

Figure 2.1: A plot of the density function $p_{\mathbf{w},m}(t)$ (defined in Corollary 2.4.0.1) of the algebraic numbers α of degree $2m$ on the unit circle w.r.t. height function $h_{\mathbf{w}}$ with weights $\mathbf{w} = \left(\binom{2m}{k}^{-1/2}\right)_{k=0}^{n}$: a) $m = 3$; b) $m = 4$; c) $m = 5$; d) $m = 7$.

and for $m = 2k+1$ *defined as*

$$\begin{cases} w_{2(k-j)} = \left(2 \cdot 4^{-k-1} \sum\limits_{i=0}^{k-j} \binom{2k+1}{2i}\binom{2k-2i+1}{k-i-j}(2a)^{2i}\right)^{-1/2}, & 0 \le j \le k; \\ w_{2(k-j)+1} = \left(2 \cdot 4^{-k} \sum\limits_{i=0}^{k-j} \binom{2k+1}{2i+1}\binom{2k-2i}{k-i-j}(2a)^{2i+1}\right)^{-1/2}, & 0 \le j \le k; \end{cases} \tag{2.4.2}$$

where $a \in \mathbb{R}_+$ *is an fixed number. Then for any integer* $m \ge 1$ *we have*

$$p_{\mathbf{w},m}(t) = \frac{1}{\pi}\left(\frac{m\left(d_a^{m-1} - s_a^{m-1}\cos 2t - s_a^{m-2}(\sin 2t)^2\right)}{d_a^m + s_a^m} + \frac{m^2 d_a^m s_a^{m-2}(\sin 2t)^2}{\left(d_a^m + s_a^m\right)^2}\right)^{1/2},$$

where $s_a = \cos(2t) + a$ *and* $d_a = 1 + a$.

2.5 Proof of Theorem 2.3.2

To prove Theorem 2.3.2 we will use the method described in Section 2.1, namely we will reduce our problem to determining the density of zeroes of some random trigonometric polynomial. The main ingredient of the further proof is the result of

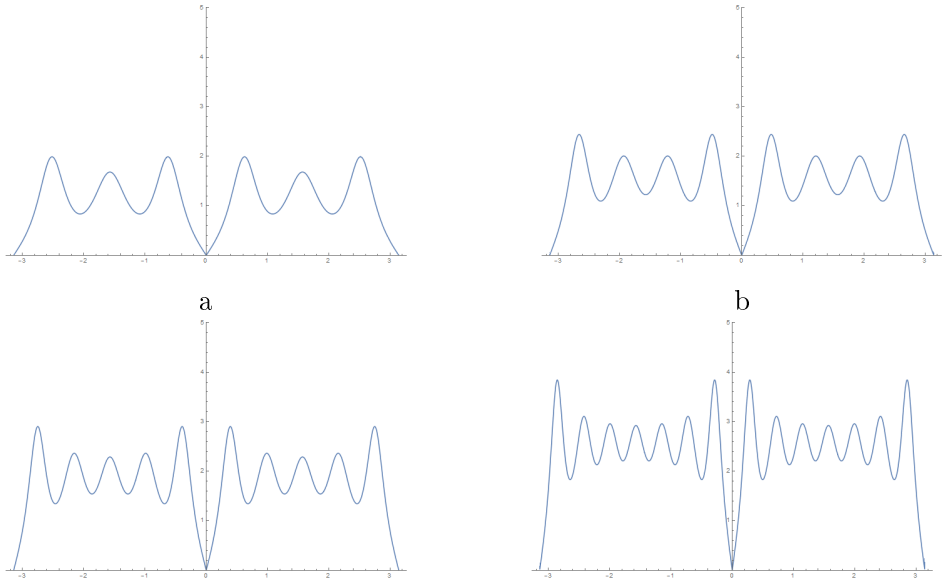

Figure 2.2: A plot of the density function $p_{\mathbf{w},m}(t)$ (defined in Corollary 2.4.0.2) of the algebraic numbers α of degree $2m$ on the unit circle w.r.t. height function $h_{\mathbf{w}}$ with weights $\mathbf{w} = (1, \dots, 1)$: a) $m = 3$; b) $m = 4$; c) $m = 5$; d) $m = 7$.

Edelman-Kostlan (see Lemma B.0.4) and the representation of the uniform distribution in the $(n+1)$-dimensional unit ball in terms of independent standard Gaussian random variables (see Lemma B.0.5).

Main Part

Consider the following class of symmetric polynomials of even degree $n = 2m$

$$\mathcal{SP}_m := \left\{ P \in \mathbb{Z}[t] \colon P(t) = \sum_{i=0}^{2m} a_i t^i,\ a_i = a_{2m-i} \right\}.$$

Let us define the subclass of symmetric polynomials of even degree $n = 2m$ and bounded elliptic height

$$\mathcal{SP}_{m,\mathbf{w}}(Q) := \mathcal{SP}_m \cap \mathcal{P}_{n,\mathbf{w}}(Q),$$

and subclass of prime symmetric polynomials of even degree $n = 2m$ and bounded elliptic height

$$\mathcal{SP}^*_{m,\mathbf{w}}(Q) := \mathcal{SP}_m \cap \mathcal{P}^*_{n,\mathbf{w}}(Q).$$

According to Proposition 2.3.1 the set of all minimal polynomials of algebraic numbers $\alpha \in \mathbb{T}$ having degree $2m$ and $h_{\mathbf{w}}(\alpha) \le Q$ coincides with $\mathcal{SP}^*_{m,\mathbf{w}}(Q)$ and, hence, we can restrict ourselves to this case only.

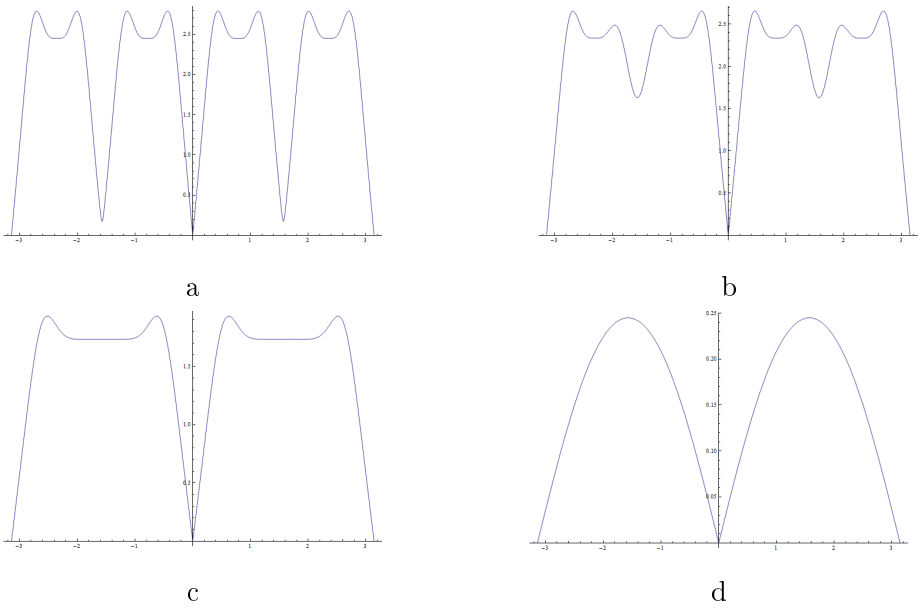

Figure 2.3: A plot of the density function $p_{\mathbf{w},m}(t)$ (defined in Corollary 2.4.0.3) of the algebraic numbers α of degree 12 on the unit circle w.r.t. height function $h_{\mathbf{w}}$ with weights defined by (2.4.1): a) $a = 0.001$; b) $a = 0.1$; c) $a = 1$; d) $a = 100$.

Given a function $F : \mathbb{C} \to \mathbb{R}$ and some Borel subset $B \subset \mathbb{C}$ denote by $\mu_F(B)$ the number of zeroes of function F lying in B. Thus, we have

$$\mathcal{N}_{2m,\mathbf{w}}(Q, \beta_1, \beta_2) = \sum_{P \in \mathcal{SP}^*_{m,\mathbf{w}}(Q)} \mu_P\left(\mathbb{T}_{\beta_1,\beta_2}\right)$$

and, since $\mu_P\left(\mathbb{T}_{\beta_1,\beta_2}\right) \leq 2m$, we can write

$$\mathcal{N}_{2m,\mathbf{w}}(Q, \beta_1, \beta_2) = \sum_{l=0}^{2m} l \cdot \#\left\{P \in \mathcal{SP}^*_{m,\mathbf{w}}(Q) \colon \mu_P\left(\mathbb{T}_{\beta_1,\beta_2}\right) = l\right\}. \tag{2.5.1}$$

Our aim is to estimate the number of the irreducible primitive symmetric polynomials having the prescribed number of the roots on the arc $\mathbb{T}_{\beta_1,\beta_2}$. Identifying polynomials with the vectors of their coefficients we reduce our problem to counting integer points in multidimensional regions.

For $l = 0, 1, \ldots, 2m$ denote by $A_l \subset \mathbb{R}^m$ the set of points $(a_0, \ldots, a_m)$ such that the polynomial $P(t) = a_0 t^{2m} + \ldots + a_m t^m + \ldots + a_0$ satisfies $\mu_P(\mathbb{T}_{\beta_1,\beta_2}) = l$ and $h_{\mathbf{w}}(P) \leq 1$. The latter condition is equivalent to the fact that vector $(a_0, \ldots, a_m)$ belongs to the ellipsoid $\mathcal{E}_{\mathbf{w}}$ defined as

$$\mathcal{E}_{\mathbf{w}} := \left\{(a_0, \ldots, a_m) \in \mathbb{R}^{m+1} \colon \frac{a_m^2}{w_m^{-2}} + 2\sum_{k=0}^{m-1} \frac{a_k^2}{w_k^{-2}} \leq 1\right\}$$

with

$$\operatorname{vol}(\mathcal{E}_{\mathbf{w}}) = \frac{\operatorname{vol}(\mathbb{B}^{m+1})}{2^{m/2} w_0 \ldots w_m}. \tag{2.5.2}$$

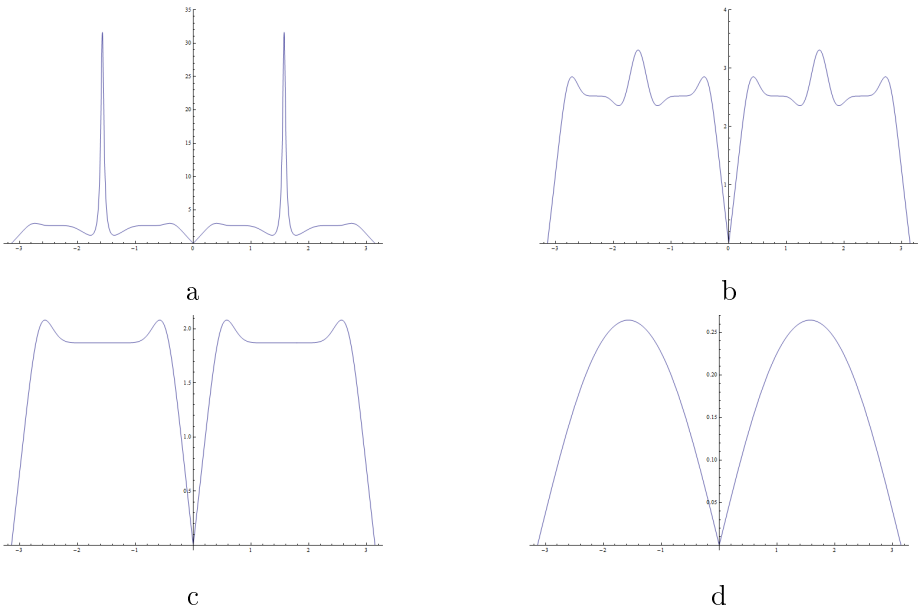

Figure 2.4: A plot of the density function $p_{\mathbf{w},m}(t)$ (defined in Corollary 2.4.0.3) of the algebraic numbers α of degree 14 on the unit circle w.r.t. height function $h_{\mathbf{w}}$ with weights defined by (2.4.2): a) $a = 0.001$; b) $a = 0.1$; c) $a = 1$; d) $a = 100$.

Then by definition of primitive polynomial we have

$$\mu^*(QA_l) = \#\{P \in \mathcal{SP}_{m,\mathbf{w}}(Q) \colon P \text{ is primitive, } \mu_P(\mathbb{T}_{\beta_1,\beta_2}) = l\},$$

where $\mu^*(D)$ denotes the number of points with co-prime integer coordinates inside some bounded set $D \subset \mathbb{R}^{m+1}$. This implies

$$\left|\frac{1}{2}\,\mu^*(Q\,A_l) - \#\{P \in \mathcal{SP}^*_{m,\mathbf{w}}(Q) : \mu_P(\mathbb{T}_{\beta_1,\beta_2}) = l\}\right| \le \mathcal{SR}_{\mathbf{w}}(m,Q), \qquad (2.5.3)$$

where $\mathcal{SR}_{\mathbf{w}}(m,Q)$ is the number of all polynomials $P \in \mathcal{SP}_{m,\mathbf{w}}(Q)$ reducible in $\mathcal{SP}_m$ (i.e. which can be written as a product of two symmetric polynomials of positive degree). The factor $1/2$ in (2.5.3) is due to the positiveness of the leading coefficient of a prime polynomial.

Our next step is to estimate the values $\mu^*(Q\,A_l)$ and $\mathcal{SR}_{\mathbf{w}}(m,Q)$. In order to estimate the first value we are going to use Lemma A.2.8. For this we need to make sure that for any $0 \le l \le 2m$ the boundary of A_l is of Lipschitz class (see Definition A.2.6).

Lemma 2.5.1. *For any $0 \le l \le 2m$ the boundary ∂A_l of the set A_l belongs to Lipschitz class $\mathrm{Lip}(m+1, M, L)$ for some constants M, L depending on l and $\mathbf{w}$ only.*

This lemma is a slightly modified and simplified version of [37, Lemma 6.4]. We give a detailed proof later in this section.

The upper bound for the number of reducible symmetric polynomials $\mathcal{SR}_{\mathbf{w}}(m,Q)$ is established in the following lemma.

Lemma 2.5.2. *For any $m \geq 2$ and any vector of positive weights $\mathbf{w}$ we have*

$$\mathcal{SR}_{\mathbf{w}}(m,Q) \ll Q^m \ (\log Q)^{\lfloor 2/m \rfloor},$$

where the constants in Vinogradov symbol depend on m and $\mathbf{w}$ only.

The proof of Lemma 2.5.2 is given below.

Now due to Lemma 2.5.1 we can apply Lemma A.2.8 to the set A_l which together with (2.5.3) and Lemma 2.5.2 gives

$$\#\{P \in \mathcal{SP}^*_{m,\mathbf{w}}(Q)\colon \mu_P(\mathbb{T}_{\beta_1,\beta_2}) = l\} = \frac{\mathrm{vol}(A_l)}{2\zeta(m+1)} Q^{m+1} + O\left(Q^m \ (\log Q)^{\lfloor 2/m \rfloor}\right),$$

and, by (2.5.1) we obtain

$$\mathcal{N}_{2m,\mathbf{w}}(Q,\beta_1,\beta_2) = \frac{Q^{m+1}}{2\zeta(m+1)} \sum_{l=0}^{2m} l \ \mathrm{vol}(A_l) + O\left(Q^m \ (\log Q)^{\lfloor 2/m \rfloor}\right). \tag{2.5.4}$$

To estimate the sum on the right side of (2.5.4) consider the random polynomial

$$G(t) := \sum_{k=0}^{m-1} \xi_k (t^k + t^{2m-k}) + \xi_m t^m,$$

where the random vector $\left(\sqrt{2}w_0\xi_0, \dots, \sqrt{2}w_{m-1}\xi_{m-1}, w_m\xi_m\right)$ is uniformly distributed over the $(m+1)$-dimensional unit ball $\mathbb{B}^{m+1}$. Then by definition of the region A_l and since the semi-axes of $\mathcal{E}_{\mathbf{w}}$ are $(\sqrt{2}\,w_0)^{-1}, \dots, (\sqrt{2}\,w_{m-1})^{-1}, w_m^{-1}$, we have

$$\mathbb{P}\left[\mu_G(\mathbb{T}_{\beta_1,\beta_2}) = l\right] = \frac{\mathrm{vol}(A_l)}{\mathrm{vol}(\mathcal{E}_{\mathbf{w}})}. \tag{2.5.5}$$

Taking $z = e^{i\theta} \in \mathbb{T}$ and using Euler's formula transform $G(z)$ as follows

$$\begin{aligned} G(z) &= \sum_{k=0}^{m-1} \xi_k (e^{ik\theta} + e^{i(2m-k)\theta}) + \xi_m e^{im\theta} \\ &= 2e^{im\theta} \left(\sum_{k=0}^{m-1} \xi_k \frac{e^{-i(m-k)\theta} + e^{i(m-k)\theta}}{2} + \frac{\xi_m}{2} \right) \\ &= 2e^{im\theta} \left(\sum_{k=1}^{m} \xi_{m-k} \cos(k\theta) + \frac{\xi_m}{2} \right) =: 2e^{im\theta}\, T(\theta). \end{aligned}$$

From this we see that the distribution of zeroes of the random polynomial $G(z)$ on the complex unit circle coincides with the distribution of zeroes of the random trigonometric polynomial $T(\theta)$ on the interval $[0, 2\pi]$ and

$$\mathbb{P}\left[\mu_G(\mathbb{T}_{\beta_1,\beta_2}) = l\right] = \mathbb{P}\left[\mu_T([\beta_1,\beta_2]) = l\right].$$

The probability on the left-hand side is difficult to calculate because of the dependency of the coefficients of T. However, by proper normalization (which does not affect the roots) we can achieve their independence.

Let $\eta_0, \dots, \eta_m$ be i.i.d. real-valued standard Gaussian random variables and let Z be a standard exponential random variable. By Lemma B.0.5 the random vector

$$\frac{(\eta_0, \eta_1, \dots, \eta_n)}{\left(\sum_{i=0}^{n} \eta_i^2 + Z\right)^{1/2}}$$

is uniformly distributed in the unit ball $\mathbb{B}^{m+1}$, that is, has the same distribution as the vector $\left(\sqrt{2}w_0\xi_0, \dots, \sqrt{2}w_{m-1}\xi_{m-1}, w_m\xi_m\right)$. Thus,

$$\frac{\left(\left(\sqrt{2}\, w_0\right)^{-1} \eta_0, \dots, \left(\sqrt{2}\, w_{m-1}\right)^{-1} \eta_{m-1}, w_m^{-1}\eta_n\right)}{\left(\sum_{i=0}^{n} \eta_i^2 + Z\right)^{1/2}} \stackrel{d}{=} (\xi_0, \dots, \xi_m).$$

Since dividing a polynomial by a non-zero constant does not affect its roots, the polynomials $T(\theta)$ and

$$\tilde{T}(\theta) := \frac{\eta_m}{2\, w_m} + \sum_{k=1}^{m} \frac{\eta_{m-k}}{\sqrt{2}\, w_{m-k}} \cos k\theta$$

have the same distribution of zeroes and

$$\mathbb{P}\left[\mu_T\left([\beta_1, \beta_2]\right) = l\right] = \mathbb{P}\left[\mu_{\tilde{T}}\left([\beta_1, \beta_2]\right) = l\right].$$

Combining this with (2.5.5) and (2.5.2), we arrive at

$$\begin{aligned}\sum_{l=0}^{2m} l\, \mathrm{vol}(A_l) &= \mathrm{vol}\left(\mathcal{E}_{\mathbf{w}}\right) \sum_{l=0}^{2m} l\, \mathbb{P}[\mu_{\tilde{T}}\left([\beta_1, \beta_2]\right) = l] \\ &= \frac{\mathrm{vol}(\mathbb{B}^{m+1})}{2^{m/2} w_0 \cdots w_m}\, \mathbb{E}\left[\mu_{\tilde{T}}\left([\beta_1, \beta_2]\right)\right].\end{aligned}$$

Finally, applying Lemma B.0.4 to the random function $\tilde{T}$ with vector $\mathbf{v}(t) = \left(\frac{1}{2}, \cos(t), \dots, \cos(mt)\right)$ and covariance matrix $C = \mathrm{Diag}\left\{w_m^{-2}, \left(\sqrt{2}\, w_{m-1}\right)^{-2}, \dots, \left(\sqrt{2}\, w_0\right)^{-2}\right\}$, we get

$$\mathbb{E}\left[\mu_{\tilde{T}}\left([\beta_1, \beta_2]\right)\right] = \int_{\beta_1}^{\beta_2} p_{\mathbf{w},m}(t)\, dt,$$

where

$$\begin{aligned}p_{\mathbf{w},m}(t) &= \frac{1}{\pi}\left[\frac{\partial^2}{\partial x \partial y} \log\left(\frac{w_m^{-2}}{4} + \frac{1}{2}\sum_{k=1}^{m} w_{m-k}^{-2} \cos(kx)\cos(ky)\right)\Big|_{x=y=t}\right]^{1/2} \\ &= \frac{1}{\pi}\left[\frac{\partial^2}{\partial x \partial y} \log\left(\frac{w_m^{-2}}{2} + \sum_{k=1}^{m} w_{m-k}^{-2} \cos(kx)\cos(ky)\right)\Big|_{x=y=t}\right]^{1/2},\end{aligned}$$

which together with (2.5.4) finishes the proof.

Proof of Lemma 2.5.1

Recall that $A_l \subset \mathbb{R}^{m+1}$ is the set of points $(a_0, \dots, a_m) \in \mathcal{E}_{\mathbf{w}}$ such that the polynomial $P(z) = a_0 z^{2m} + \dots + a_m z^m + \dots + a_0$ satisfies $\mu_P(\mathbb{T}_{\beta_1,\beta_2}) = l$. For $z = e^{i\theta}$ we have

$$P(z) = 2e^{im\theta}\left(\sum_{k=1}^{m} a_{m-k}\cos(k\theta) + \frac{a_m}{2}\right) =: 2e^{im\theta}\tilde{T}(\theta),$$

and, hence, A_l is a set of points $(a_0, \dots, a_m) \in \mathcal{E}_{\mathbf{w}}$ such that the trigonometric polynomial $\tilde{T}$ satisfies $\mu_{\tilde{T}}([\beta_1, \beta_2]) = l$.

The boundary of A_l is contained in the union of three sets:

1. the boundary of $\mathcal{E}_{\mathbf{w}}$;
2. the set
$$A' = \left\{(a_0, \dots, a_m) \in \mathcal{E}_{\mathbf{w}} : \tilde{T}(\beta_1) = 0 \quad \text{or} \quad \tilde{T}(\beta_2) = 0\right\};$$
3. the set A'' of points $(a_0, \dots, a_m) \in \mathcal{E}_{\mathbf{w}}$ such that the trigonometric polynomial $\tilde{T}$ has double real roots in $[\beta_1, \beta_2]$.

Thus, it is enough to show that each of these sets is of Lipschitz class.

(i) The boundary of $\mathcal{E}_{\mathbf{w}}$. Since $\mathcal{E}_{\mathbf{w}}$ is a convex bounded body, by Theorem A.2.9 its boundary belongs to the Lipschitz class.

(ii) The set A'. Without loss of generality let $\tilde{T}(\beta_1) = 0$, which is equivalent to

$$a_m = -2\sum_{k=1}^{m} a_{m-k}\cos(k\beta_1).$$

Since $(a_0, \dots, a_m) \in \mathcal{E}_{\mathbf{w}}$, there exists a constant $C := \max_i w_i^{-1}$ such that $a_0, \dots, a_{m-1} \le C$. Consider a Lipschitz map $\phi = (\phi_0, \dots, \phi_m) : [0,1]^m \to \mathbb{R}^{m+1}$ defined as

$$\phi_i(t_0, \dots, t_{m-1}) = Ct_i, \quad i = 0, \dots, m-1,$$

and

$$\phi_m(t_0, \dots, t_{m-1}) = -2C\sum_{k=1}^{m} t_{m-k}\cos(k\beta_1).$$

We obviously have

$$a_i = \phi_i(a_0/C, \dots, a_{m-1}/C), \quad i = 0, \dots, m-1,$$

which implies $A' \subset \phi([0,1]^m)$. Therefore A' is of Lipschitz class.

(iii) The set A''. Suppose that $(a_0, \dots, a_m) \in A''$. Then $\tilde{T}(\theta)$ has a multiple real root, say β_0, which implies

$$\tilde{T}(\beta_0) = 0, \quad \tilde{T}'(\beta_0) = 0, \tag{2.5.6}$$

or (excluding the trivial case $\beta_0 = 0$), equivalently,

$$a_{m-1} = -\sum_{k=2}^{m} k a_{m-k} \frac{\sin(k\beta_0)}{\sin\beta_0},$$

$$a_m = -2\sum_{k=2}^{m} a_{m-k}\cos(k\beta_0) + 2\cot\beta_0 \sum_{k=2}^{m} k a_{m-k}\sin(k\beta_0).$$

Again, there exists a constant $C := \max\limits_i w_i^{-1}$ such that $a_0, \ldots, a_{m-2} \le C$. Moreover, we have $|\beta_0| \le \pi$. Consider a map $\phi = (\phi_0, \ldots, \phi_m) : [0,1]^m \to \mathbb{R}^{m+1}$ defined as

$$\phi_i(t, t_0, \ldots, t_{m-2}) = Ct_i, \quad i = 0, \ldots, m-2,$$

$$\phi_{m-1}(t, t_0, \ldots, t_{m-2}) = -C\sum_{k=2}^{m} k t_{m-k} \frac{\sin(k\pi t)}{\sin(\pi t)},$$

and

$$\phi_m(t, t_0, \ldots, t_{m-2}) = -2C\sum_{k=2}^{m} t_{m-k}\cos(k\pi t) + 2C\cot(\pi t)\sum_{k=2}^{m} k t_{m-k}\sin(k\pi t).$$

Since ϕ is continuously differentiable in a compact, it satisfies the Lipschitz condition. We obviously have

$$a_i = \phi_i(\beta_0/\pi, a_0/C, \ldots, a_{m-2}/C), \quad i = 0, \ldots, m,$$

which implies $A'' \subset \phi([0,1]^m)$. Therefore A'' is of Lipschitz class.

Proof of Lemma 2.5.2

To prove this lemma we will use the method of [45].

Consider some polynomial $P(t) = a_n t^n + \ldots + a_1 t + a_0$. Denote by $\mathcal{SR}_H(m, Q)$ the number of symmetric reducible polynomials $P \in \mathcal{SP}_m$ of even degree $n = 2m$ and bounded 'naïve' height $H(P) \le Q$. Using the inequality

$$H(\alpha) \le \left(\min_{0\le i\le m} |w_i|\right)^{-1} h_{\mathbf{w}}(\alpha),$$

which follows from generalized mean inequality, we conclude, that

$$\mathcal{SR}_{\mathbf{w}}(m, Q) \le \mathcal{SR}_H\left(m, \left(\min_{0\le i\le n} w_i\right)^{-1} Q\right) \tag{2.5.7}$$

and the problem reduces to estimating the value $\mathcal{SR}_H(m, Q)$.

Denote by $R_m^2(T)$ the number of pairs (P_1, P_2) of symmetric polynomials with integer coefficients such that $\deg P_1 + \deg P_2 = 2m$ and

$$H(P_1)\, H(P_2) \le T.$$

Then by equation (A.1.5) from Lemma A.1.17 it is easy to see

$$R_m^2(Q_1) \geq \mathcal{SR}_H(m, Q), \tag{2.5.8}$$

where $Q_1 = \left(2^{2m-2}\sqrt{2m+1}\right) Q$. Since, obviously,

$$\#\{P \in \mathcal{SP}_k \colon H(P) = q\} \leq 2(k+1)(2q+1)^k \ll q^k,$$

then we get

$$R_m^2(T) \ll \sum_{k=1}^{m-1} \sum_{\substack{x,y \in \mathbb{Z}, x,y \geq 1, \\ xy \leq T}} x^k y^{m-k} \ll T^m (\log T)^{\lfloor 2/m \rfloor}.$$

For the proof of this estimate we refer the reader to [45, eq. (3.2)]. Using the above estimate and inequalities (2.5.7), (2.5.8) we obtain

$$\begin{aligned}\mathcal{SR}_{\mathbf{w}}(m, Q) &\leq \mathcal{SR}_H\left(m, \left(\min_{0 \leq i \leq n} w_i\right)^{-1} Q\right) \\ &\leq R_m^2\left(\left(\min_{0 \leq i \leq n} w_i\right)^{-1} Q_1\right) \ll Q^m (\log Q)^{\lfloor 2/m \rfloor},\end{aligned}$$

where the constants in Vinogradov symbol depend on m and $\mathbf{w}$ only. This completes the proof.

2.6 Proofs of Corollaries

Proof of Corollary 2.4.0.1

Consider the function $p_{\mathbf{w},m}(t)$ defined by equation (2.3.1) with weights $\mathbf{w} = \left(\binom{2m}{k}^{-1/2}\right)_{k=0}^{2m}$. Write the kernel

$$\begin{aligned}K_{\mathbf{w},m}(x, y) &:= \frac{w_m^{-2}}{2} + \sum_{k=1}^{m} w_{m-k}^{-2} \cos(kx)\cos(ky) \\ &= \frac{1}{2}\binom{2m}{m} + \sum_{k=1}^{m} \binom{2m}{m-k} \cos(kx)\cos(ky)\end{aligned}$$

and, using Euler's formula, transform it as follows

$$\begin{aligned}K_{\mathbf{w},m}(x, y) &= \frac{1}{2}\binom{2m}{m} + \sum_{k=1}^{m} \binom{2m}{m-k} \frac{e^{-ikx} + e^{ikx}}{2} \frac{e^{-iky} + e^{iky}}{2} \\ &= \frac{e^{-im(x+y)}}{4}\left(\sum_{k=0}^{2m}\binom{2m}{k} e^{ik(x+y)} + \sum_{k=0}^{2m}\binom{2m}{k} e^{iky} e^{i(2m-k)x}\right) \\ &= \frac{e^{-im(x+y)}}{4}\left(\left(1 + e^{i(x+y)}\right)^{2m} + \left(e^{iy} + e^{ix}\right)^{2m}\right).\end{aligned}$$

Substituting the above expression into (2.3.1) we get

$$\begin{aligned}
p_{\mathbf{w},m}(t) &= \frac{1}{\pi}\left[\frac{\partial^2}{\partial x\partial y}\log K_{\mathbf{w},m}(x,y)\Big|_{x=y=t}\right]^{1/2} \\
&= \frac{1}{\pi}\left[\frac{\partial^2}{\partial x\partial y}\Big(-\log 4 - im(x+y) + \log 4e^{im(x+y)}K_{\mathbf{w},m}(x,y)\Big)\Big|_{x=y=t}\right]^{1/2} \\
&= \frac{1}{\pi}\left[\frac{\partial^2}{\partial x\partial y}\log \tilde{K}_m(x,y)\Big|_{x=y=t}\right]^{1/2} \\
&= \frac{1}{\pi}\left[\frac{\tilde{K}_m(t,t)\cdot \frac{\partial^2}{\partial x\partial y}\tilde{K}_m(x,y)\big|_{x=y=t} - \frac{\partial}{\partial x}\tilde{K}_m(x,t)\big|_{x=t}\cdot\frac{\partial}{\partial y}\tilde{K}_m(t,y)\big|_{y=t}}{\tilde{K}_m^2(t,t)}\right]^{1/2},
\end{aligned}$$

where $\tilde{K}_m(x,y) = \left(1+e^{i(x+y)}\right)^{2m} + \left(e^{iy}+e^{ix}\right)^{2m}$. The task is to find the partial derivatives of the function $\tilde{K}_m(x,y)$ for $x=y=t$. Using Euler's formula, we get

$$\tilde{K}_m(t,t) = \left(1+e^{2it}\right)^{2m} + 2^{2m}e^{2imt} = 2^{2m}e^{2imt}\left((\cos t)^{2m}+1\right); \tag{2.6.1}$$

$$\begin{aligned}
\frac{\partial}{\partial x}\tilde{K}_m(x,t)\big|_{x=t} = \frac{\partial}{\partial y}\tilde{K}_m(t,y) &= 2ime^{2it}\left(1+e^{2it}\right)^{2m-1} + 2im\,2^{2m-1}e^{2imt} \\
&= 2im\,2^{2m-1}e^{2imt}\left(e^{it}(\cos t)^{2m-1}+1\right);
\end{aligned} \tag{2.6.2}$$

$$\begin{aligned}
\frac{\partial^2}{\partial x\partial y}\tilde{K}_m(x,y)\big|_{x=y=t} &= -2me^{2it}\left(1+e^{2it}\right)^{2m-1} - 2m(2m-1)e^{4it}\left(1+e^{2it}\right)^{2m-2} \\
&\quad - 2m(2m-1)\,2^{2m-2}e^{2imt} = -2m\,2^{2m-2}e^{2imt}\Big(2e^{it}(\cos t)^{2m-1} \\
&\quad + (2m-1)e^{2it}(\cos t)^{2m-2} + (2m-1)\Big).
\end{aligned} \tag{2.6.3}$$

Thus, by equations (2.6.1), (2.6.2) and (2.6.3) we obtain

$$\begin{aligned}
p_{\mathbf{w},m}(t) = \sqrt{\frac{m}{2\pi^2}}&\left((\cos t)^{2m}+1\right)^{-1}\cdot\Big(e^{2it}(\cos t)^{4m-2} - 2e^{it}(\cos t)^{4m-1} \\
&- (2m-1)(\cos t)^{2m} - (2m-1)e^{2it}(\cos t)^{2m-2} + (2m-1)e^{it}(\cos t)^{2m-1} + 1\Big)^{1/2}.
\end{aligned}$$

Using the equalities

$$\begin{aligned}
e^{it} &= \cos t + i\sin t; \\
e^{2it} &= \cos(2t) + i\sin(2t) = 2(\cos t)^2 - 1 + 2i\sin t\cos t.
\end{aligned}$$

we have

$$p_{\mathbf{w},m}(t) = \sqrt{\frac{m}{2\pi^2}} \cdot \frac{\left(1-(\cos^2 t)^{2m-1} + (2m-1)(\cos t)^{2m-2}\ \left(1-\cos^2 t\right)\right)^{1/2}}{(\cos t)^{2m}+1}$$
$$= \sqrt{\frac{m}{2\pi^2}} \cdot \frac{\sqrt{1-\cos^2 t}\ \left(\sum_{k=0}^{2m-2}(\cos t)^{2k} + (2m-1)\,(\cos t)^{2m-2}\right)^{1/2}}{(\cos t)^{2m}+1}$$
$$= \sqrt{\frac{m}{2\pi^2}} \cdot \frac{|\sin t|\ \left(\sum_{k=0}^{2m-2}(\cos t)^{2k} + (2m-1)\,(\cos t)^{2m-2}\right)^{1/2}}{(\cos t)^{2m}+1}.$$

Proof of Corollary 2.4.0.2

Before we start recall some trigonometric formulas which will be used in our calculations

$$\frac{\sin\left((N+\frac{1}{2})(x-y)\right)}{\sin\frac{x-y}{2}} = 1 + 2\sum_{k=1}^{N}\cos(k(x-y));$$

$$\sin\left(\frac{N(x-y)}{2}\right) = \sum_{k\ \text{odd}}(-1)^{(k-1)/2}\binom{N}{k}\left(\cos\frac{x-y}{2}\right)^{N-k}\left(\sin\frac{x-y}{2}\right)^{k};$$

$$\cos\left(\frac{N(x-y)}{2}\right) = \sum_{k\ \text{even}}(-1)^{k/2}\binom{N}{k}\left(\cos\frac{x-y}{2}\right)^{N-k}\left(\sin\frac{x-y}{2}\right)^{k}.$$

Consider the function $p_{\mathbf{w},m}(t)$ with weights $\mathbf{w} = (1,\dots,1)$. In this case the kernel has the form

$$K_{\mathbf{w},m}(x,y) = \frac{1}{2} + \sum_{k=1}^{m}\cos(kx)\cos(ky) = \frac{1}{4} + \sum_{k=1}^{m}\left(\frac{1}{2}\cos k(x+y) + \frac{1}{2}\cos k(x-y)\right)$$
$$= \frac{1}{2} + \frac{1}{2}\sum_{k=1}^{m}\cos k(x+y) + \frac{1}{2}\sum_{k=1}^{m}\cos k(x-y)$$
$$= \frac{\sin\left((m+\frac{1}{2})(x+y)\right)}{4\sin\frac{x+y}{2}} + \frac{\sin\left((m+\frac{1}{2})(x-y)\right)}{4\sin\frac{x-y}{2}}.$$

It should be noted that $\frac{\sin\left((m+\frac{1}{2})t\right)}{\sin\frac{t}{2}}$ is the well-known Dirichlet kernel.

Expression (2.3.1) can be written as

$$p_{\mathbf{w},m}(t) = \frac{1}{\pi}\left[\frac{K_{\mathbf{w},m}(t,t)\cdot\frac{\partial^2}{\partial x\partial y}K_{\mathbf{w},m}(x,y)\big|_{x=y=t} - \frac{\partial}{\partial x}K_{\mathbf{w},m}(x,t)\big|_{x=t}\cdot\frac{\partial}{\partial y}K_{\mathbf{w},m}(t,y)\big|_{y=t}}{K^2_{\mathbf{w},m}(t,t)}\right]^{1/2}.$$

In order to determine the function $p_{\mathbf{w},m}(t)$ it is necessary to find the partial derivatives of the function $K_{\mathbf{w},m}(x,y)$ for $x = y = t$.

Recall that $b_m = 2m+1$. Thus, we have

$$K_{\mathbf{w},m}(t,t) = \frac{\sin(b_m t)}{4\sin t} + \frac{\sin\left((m+\frac{1}{2})(x-y)\right)}{4\sin\frac{x-y}{2}}\Big|_{x=y=t} = \frac{b_m}{4} + \frac{\sin(b_m t)}{4\sin t};$$

$$\begin{aligned}
\frac{\partial}{\partial x}K_{\mathbf{w},m}(x,t)\Big|_{x=t} &= \frac{\partial}{\partial y}K_{\mathbf{w},m}(t,y)\Big|_{y=t} \\
&= \left(\frac{m\cos\frac{b_m(x-y)}{2})}{4\sin\frac{x-y}{2}} - \frac{\sin\frac{2m(x-y)}{2}}{8\sin^2\frac{x-y}{2}}\right)\Big|_{x=y=t} + \frac{m\cos(b_m t)}{4\sin t} - \frac{\sin(2mt)}{8\sin^2 t} \\
&= \frac{m}{4\sin\frac{x-y}{2}}\Big|_{x=y=t} - \frac{m}{4\sin\frac{x-y}{2}}\Big|_{x=y=t} + \frac{m\cos(b_m t)}{4\sin t} - \frac{\sin(2mt)}{8\sin^2 t} \\
&= \frac{m\cos(b_m t)}{4\sin t} - \frac{\sin(2mt)}{8\sin^2 t};
\end{aligned}$$

$$\begin{aligned}
\frac{\partial^2}{\partial x\partial y}K_{\mathbf{w},m}(x,y)\Big|_{x=y=t} &= \left(\frac{m^2\sin\frac{b_m(x-y)}{2})}{4\sin\frac{x-y}{2}} + \frac{m\cos\frac{2m(x-y)}{2})}{4\sin^2\frac{x-y}{2}} - \frac{\sin\frac{2m(x-y)}{2})}{8\sin^3\frac{x-y}{2}}\right)\Big|_{x=y=t} \\
&\quad - \frac{m^2\sin(b_m t)}{4\sin t} - \frac{m\cos(2mt)}{4\sin^2 t} + \frac{\cos t\,\sin(2mt)}{8\sin^3 t} \\
&= \frac{m^2 b_m}{4} + \frac{m}{4\sin^2\frac{x-y}{2}}\Big|_{x=y=t} - \frac{m^2(2m-1)}{4} - \frac{m}{4\sin^2\frac{x-y}{2}}\Big|_{x=y=t} \\
&\quad + \frac{m(2m-1)(m-1)}{2} - \frac{m^2\sin(b_m t)}{4\sin t} - \frac{m\cos(2mt)}{4\sin^2 t} + \frac{\cos t\,\sin(2mt)}{8\sin^3 t} \\
&= \frac{\cos t\,\sin(2mt)}{8\sin^3 t} - \frac{m^2\sin(b_m t)}{4\sin t} - \frac{m\cos(2mt)}{4\sin^2 t} + \frac{(m^2+m)b_m}{12}.
\end{aligned}$$

Using the above equations we obtain

$$\begin{aligned}
p_{\mathbf{w},m}(t) = \frac{1}{\pi}\left(b_m + \frac{\sin(b_m t)}{\sin t}\right)^{-1} \cdot \Big(&\frac{b_m\sin(b_m t)}{2(\sin t)^3} - \frac{b_m^2}{2}\frac{\cos(b_m t)\cos t}{(\sin t)^2} \\
&+ \frac{(\sin(b_m t))^2}{4(\sin t)^4} - \frac{b_m^3+2b_m}{6}\frac{\sin(b_m t)}{\sin t} - \frac{b_m^2}{4(\sin t)^2} + \frac{(m^2+m)b_m^2}{3}\Big)^{1/2},
\end{aligned}$$

Proof of Corollary 2.4.0.3

In order to calculate the density $p_{\mathbf{w},m}(t)$ in this case we will use the following trigonometric identities for integer $k \geq 0$

$$(\cos t)^{2k} = 2^{-2k}\binom{2k}{k} + 2^{-2k+1}\sum_{j=0}^{k-1}\binom{2k}{j}\cos(2k-2j)t, \tag{2.6.4}$$

$$(\cos t)^{2k+1} = 2^{-2(k+1)}\sum_{j=0}^{k}\binom{2k+1}{j}\cos(2k+1-2j)t. \tag{2.6.5}$$

Consider the function $p_{\mathbf{w},m}(t)$ defined by equation (2.3.1) with weights $\mathbf{w}$ defined by (2.4.1) and (2.4.2). In this case the kernel has the following form

$$\begin{aligned}K_{\mathbf{w},m}(x,y) &= \frac{w_m^{-2}}{2} + \sum_{i=1}^{m} w_{m-i}^{-2}\cos(ix)\cos(iy)\\ &= \frac{w_m^{-2}}{2} + \sum_{i=1}^{m} \frac{w_{m-i}^{-2}}{2}\left(\cos i(x+y) + \cos i(x-y)\right)\\ &= \left(\frac{w_m^{-2}}{4} + \sum_{i=1}^{m} \frac{w_{m-i}^{-2}}{2}\cos i(x-y)\right) + \left(\frac{w_m^{-2}}{4} + \sum_{i=1}^{m} \frac{w_{m-i}^{-2}}{2}\cos i(x+y)\right).\end{aligned}$$

Let $m = 2k$. For any positive real a consider the expression

$$\begin{aligned}F(x,\pm y) &:= (\cos(x\pm y)+a)^m\\ &= \sum_{i=0}^{k}\binom{2k}{2i}a^{2i}\left(\cos(x\pm y)\right)^{2(k-i)} + \sum_{i=1}^{k}\binom{2k}{2i-1}a^{2i-1}\left(\cos(x\pm y)\right)^{2(k-i)+1}.\end{aligned}$$

Then, using equations 2.6.4 and 2.6.5 we get

$$\begin{aligned}&F(x,\pm y)\\ &= \frac{1}{4^k}\sum_{i=0}^{k}\binom{2k}{2i}(2a)^{2i}\left(\binom{2(k-i)}{k-i} + 2\sum_{j=0}^{k-i-1}\binom{2(k-i)}{j}\cos 2(k-i-j)(x\pm y)\right)\\ &+ \frac{1}{2\cdot 4^k}\sum_{i=1}^{k}\binom{2k}{2i-1}(2a)^{2i-1}\left(\sum_{j=0}^{k-i}\binom{2(k-i)+1}{j}\cos(2(k-i-j)+1)(x\pm y)\right).\end{aligned}$$

Rewrite this expression in the following form

$$\begin{aligned}F(x,\pm y) &= \frac{1}{4^k}\sum_{i=0}^{k}\binom{2k}{2i}\binom{2(k-i)}{k-i}(2a)^{2i}\\ &+ \frac{2}{4^k}\sum_{j=1}^{k}\sum_{i=0}^{k-j}\binom{2k}{2i}\binom{2(k-i)}{k-i-j}(2a)^{2i}\cos 2j(x\pm y)\\ &+ \frac{1}{2\cdot 4^k}\sum_{j=0}^{k-1}\sum_{i=1}^{k-j}\binom{2k}{2i-1}\binom{2(k-i)+1}{k-i-j}(2a)^{2i-1}\cos(2j+1)(x\pm y).\end{aligned}$$

Analogously for $m = 2k+1$ we get

$$\begin{aligned}F(x,\pm y) &:= (\cos(x\pm y)+a)^m\\ &= \sum_{i=0}^{k}\binom{2k+1}{2i+1}a^{2i+1}\left(\cos(x\pm y)\right)^{2(k-i)} + \sum_{i=0}^{k}\binom{2k+1}{2i}a^{2i}\left(\cos(x\pm y)\right)^{2(k-i)+1}.\end{aligned}$$

Applying 2.6.4 and 2.6.5 we obtain

$$
\begin{aligned}
&F(x,\pm y)\\
&\quad=\frac{1}{2\cdot 4^k}\sum_{i=0}^{k}\binom{2k+1}{2i+1}(2a)^{2i+1}\left(\binom{2(k-i)}{k-i}+2\sum_{j=0}^{k-i-1}\binom{2(k-i)}{j}\cos 2(k-i-j)(x\pm y)\right)\\
&\quad+\frac{1}{4^{k+1}}\sum_{i=0}^{k}\binom{2k+1}{2i}(2a)^{2i}\left(\sum_{j=0}^{k-i}\binom{2(k-i)+1}{j}\cos(2(k-i-j)+1)(x\pm y)\right).
\end{aligned}
$$

Rewrite this expression in the following form:

$$
\begin{aligned}
F(x,\pm y)=&\frac{1}{2\cdot 4^k}\sum_{i=0}^{k}\binom{2k+1}{2i+1}\binom{2(k-i)}{k-i}(2a)^{2i+1}\\
&+\frac{1}{4^k}\sum_{j=1}^{k}\sum_{i=0}^{k-j}\binom{2k+1}{2i+1}\binom{2(k-i)}{k-i-j}(2a)^{2i+1}\cos 2j(x\pm y)\\
&+\frac{1}{4^{k+1}}\sum_{i=0}^{k}\sum_{j=0}^{k}\binom{2k+1}{2i}\binom{2(k-i)+1}{k-i-j}(2a)^{2i}\cos(2j+1)(x\pm y).
\end{aligned}
$$

Then, with weights $\mathbf{w}$ defined by (2.4.1) and (2.4.2), we get

$$K_{\mathbf{w},m}(x,y)=F(x,y)+F(x,-y)=(\cos(x+y)+a)^m+(\cos(x-y)+a)^m\,.$$

In order to determine the function $p_{\mathbf{w},m}(t)$ we need to find the partial derivatives of the function $K_{\mathbf{w},m}(x,y)$ for $x=y=t$. Using the expression above and remembering that $s_a=\cos 2t+a$, $d_a=1+a$ we have

$$K_{\mathbf{w},m}(t,t)=(\cos(2t)+a)^m+(1+a)^m\,;$$

$$
\begin{aligned}
\frac{\partial}{\partial x}K_{\mathbf{w},m}(x,t)\Big|_{x=t}&=\frac{\partial}{\partial y}K_{\mathbf{w},m}(t,y)\Big|_{y=t}\\
&=\Big(-m\,(\cos(x+y)+a)^{m-1}\sin(x+y)\\
&\quad-m\,(\cos(x-y)+a)^{m-1}\sin(x-y)\Big)\Big|_{x=y=t}\\
&=-m\,s_a^{m-1}\,\sin 2t;
\end{aligned}
$$

$$
\begin{aligned}
\frac{\partial^2}{\partial x\partial y}K_{\mathbf{w},m}(x,y)\Big|_{x=y=t}&=m(m-1)\,(\cos(x+y)+a)^{m-2}\sin^2(x+y)\Big|_{x=y=t}\\
&\quad-m\,(\cos(x+y)+a)^{m-1}\cos(x+y)\Big|_{x=y=t}\\
&\quad-m(m-1)\,(\cos(x-y)+a)^{m-2}\sin^2(x-y)\Big|_{x=y=t}\\
&\quad+m\,(\cos(x+y)+a)^{m-1}\cos(x-y)\Big|_{x=y=t}\\
&=m(m-1)\,s_a^{m-2}\,(\sin 2t)^2-m\,s_a^{m-1}\,\cos 2t+m\,d_a^{m-1}.
\end{aligned}
$$

Thus, we obtain

$$p_{\mathbf{w},m}(t) = \frac{1}{\pi}\left(\frac{m\left(d_a^{m-1} - s_a^{m-1}\,\cos 2t - s_a^{m-2}\,(\sin 2t)^2\right)}{d_a^m + s_a^m} + \frac{m^2\, d_a^m\, s_a^{m-2}\,(\sin 2t)^2}{\left(d_a^m + s_a^m\right)^2}\right)^{1/2}.$$

Chapter 3

Counting Points with Algebraic Conjugate Coordinates

In this chapter we investigate the distribution of algebraic numbers with respect to 'naïve' height. Given some $Q > 0$ denote by $\mathcal{P}_n(Q)$ the following class of polynomials

$$\mathcal{P}_n(Q) = \{P \in \mathbb{Z}[t] : \deg P \leq n, H(P) \leq Q\}.$$

During this chapter we will use the notation $c_j > 0$, $j \in \mathbb{N}$ to denote the positive values which do not depend on $H(P)$ or Q. For convenience let us also define the following function

$$\omega_n(x) = \sum_{k=0}^{n-1} |x|^k.$$

3.1 Introduction

Let us start with some short historical review. The first result providing some information about the distribution of algebraic numbers was obtained in 1970 by Baker and Schmidt [2]. In order to study the distribution of algebraic numbers Baker and Schmidt introduced the concept of a regular system. A countable set $\Gamma \subset \mathbb{R}$ together with positive-valued function $N : \Gamma \to \mathbb{R}^+$ is called a *regular system* if there exists a constant $C = C(\Gamma, N) > 0$ such that for every interval $I \subset \mathbb{R}$ and a sufficiently large number $T > T_0(\Gamma, N, I) > 0$ there exist at least $C\,T\lambda_1(I)$ points $\gamma_1, \gamma_2, \ldots, \gamma_t \in \Gamma \cap I$ such that

$$\begin{aligned} N(\gamma_i) &\leq T, \quad 1 \leq i \leq t, \\ |\gamma_i - \gamma_j| &> T^{-1}, \quad 1 \leq i < j \leq t. \end{aligned} \tag{3.1.1}$$

A simple example of a regular system is the set of non-zero rational numbers p/q together with the function $N(p/q) := q^2$. An important fact is that the set $\mathbb{A}_n$ together with the function $N_1(\alpha) = H(\alpha)^{n+1} \left(\ln H(\alpha)\right)^{-3n(n+1)}$ is a regular system [2]. This result has been improved, showing that the set $\mathbb{A}_n$ together with the function $N_2(\alpha) = H(\alpha)^{n+1} \left(1 + |\alpha|\right)^{-n(n+1)}$ [7] and the set $\mathcal{O}_n$ together with the function $N_3(\alpha) = H(\alpha)^{n} \left(1 + |\alpha|\right)^{n(n-1)}$ [16] are regular systems. Moreover, the same holds for the set of algebraic numbers and algebraic integers of degree at most n.

Let us mention that these results do not provide any information about the dependence of the value $T_0(\Gamma, N, I)$ on the length of the interval I, although this is an interesting question. In his monograph [17] Bugeaud showed that $T_0(\mathbb{Q}, N, I) = 10^4(\lambda_1(I))^{-2}\left(\log(100(\lambda_1(I))^{-1})\right)^2$ (see equation (5.6)) and Beresnevich [6] calculated $T_0(\mathbb{A}_2, N_2, I) = 72^3(\lambda_1(I))^{-3}\left(\log 72(\lambda_1(I))^{-1}\right)^3$ for any interval $I \subset [0;1]$, but for arbitrary degree the question stayed open for some time.

In 2015 Bernik and Götze [14] motivated by this problem obtained the following result. Given an interval $I \subset \mathbb{R}$, denote by $\mathcal{N}_n(\mathbb{A}, Q, I)$ the number of algebraic numbers $\alpha \in I$ of degree at most n and 'naïve' height at most Q. Then for any interval I of length $\lambda_1(I) \asymp Q^{-s}$, $0 < s \leq 1$, and $Q > Q_0$ the following estimate holds

$$\mathcal{N}_n(\mathbb{A}, Q, I) \gg Q^{n+1}\lambda_1(I), \tag{3.1.2}$$

where the constants in the Vinogradov symbol and the value Q_0 depend on n and the middle point of the interval I only. To prove this inequality they basically constructed a set of algebraic numbers $\gamma_1, \gamma_2, \ldots, \gamma_t \in \mathbb{A}_n \cap I$ satisfying conditions (3.1.1) with $N(\alpha) = H(\alpha)^{n+1}$. This allowed to conclude that $T_0(\mathbb{A}_n, N_2, I) = C_1(n)(\lambda_1(I))^{-n-1}$ for any interval $I \subset [0;1]$.

The results mentioned above have many interesting applications. For example, a regular system of algebraic numbers is used to obtain lower bounds for the Hausdorff dimension of various sets of algebraic number [2, 23] and to prove Khinchine-type theorems in the case of divergence [7, 11].

In this chapter we will obtain the results similar to (3.1.2) for the set of algebraic integers and consider the two-dimensional analogue of the problem.

Given a Borel subset $D \subset \mathbb{R}^2$, consider the function $\mathcal{N}_n^2(\mathbb{A}, Q, D)$, which counts the number of ordered pairs $\boldsymbol{\alpha} := (\alpha_1, \alpha_2) \in D$ of distinct conjugate algebraic numbers α_1, α_2 of degree at most n and 'naïve' height at most Q, and the function $\mathcal{N}_n^2(\mathcal{O}, Q, D)$, which counts the number of ordered pairs $\boldsymbol{\alpha} := (\alpha_1, \alpha_2) \in D$ of distinct conjugate algebraic integers α_1, α_2 of degree n and 'naïve' height at most Q.

We will derive the upper and lower bounds for values $\mathcal{N}_n^2(\mathbb{A}, Q, D)$ and $\mathcal{N}_n^2(\mathcal{O}, Q, D)$ in case of two classes of subsets D having fixed 'position' and measure depending on Q that vanishing as Q tends to infinity. The first class of subsets under consideration are rectangles with fixed middle point, and the second class are ϵ-neighborhoods of some fixed curve. For algebraic integers we will derive upper and lower bounds for the number of algebraic integers with height at most Q lying in some interval $I \in \mathbb{R}$ with fixed middle point and length vanishing as Q tends to infinity. We will start by obtaining the estimates for the number of points with algebraic conjugate coordinates and derive the result for algebraic integers using those estimates.

3.2 Rectangles of Small Measure

Consider a rectangle $\Pi = I_1 \times I_2$ with middle point $\mathbf{d} = (d_1, d_2)$, $d_1 \neq d_2$ and sizes $\lambda_1(I_1) = c_{1,1} Q^{-s_1}$, $\lambda_1(I_2) = c_{1,2} Q^{-s_2}$. The condition $d_1 \neq d_2$ is necessary since it allows to exclude from consideration the neighborhood of the line $x = y$. The points in this area can not be well approximated by points with algebraic conjugate coordinates since algebraic conjugate numbers have some kind of repulsion [18, 28].

In this section we will prove a few theorems providing the upper and lower estimates of the value $\mathcal{N}_n^2(\mathbb{A}, Q, \Pi)$ for some choices of s_1 and s_2. Those estimates are asymptotic with $Q \to \infty$. Moreover upper and lower estimates are equal up to multiplication by the constant factor.

Let us start with lower estimates since they form the most difficult and technically involved part.

Theorem 3.2.1. *For any rectangle $\Pi = I_1 \times I_2$ with middle point $\mathbf{d} = (d_1, d_2)$, $d_1 \neq d_2$ satisfying the following conditions:*

1. *$\lambda_1(I_i) = c_{1,i} Q^{-s_i}$, where $s_i < 1$ and $0 < s_1 + s_2 \leq 1$, $i = 1, 2$;*
2. *$c_{1,1} c_{1,2} > c_0(n, \mathbf{d}) > 0$ for $s_1 + s_2 = 1$;*

any integer $n \geq 2$, and any real positive $Q > Q_0(n, \mathbf{d}, \mathbf{s})$ there exists a constant $c_2 = c_2(n, \mathbf{d}) > 0$, such that

$$\mathcal{N}_n^2(\mathbb{A}, Q, \Pi) \geq c_2 Q^{n+1} \lambda_2(\Pi). \tag{3.2.1}$$

One can not avoid the condition $s_1 + s_2 \leq 1$ since for $s_1 + s_2 > 1$ there exist rectangles Π such that the statement of Theorem 3.2.1 does not hold. The example of such rectangle is $\Pi = \left(0, 0.5\, Q^{-1}\right) \times (0, 0.5)$. It is easy to prove [14] that the interval $\left(0, 0.5\, Q^{-1}\right)$ does not contain algebraic numbers of any degree and height at most Q. It should be noted that this example is not unique and one can construct the rectangle which does not contain points with algebraic conjugate coordinates near every ration point with bounded denominators.

This simple fact shows that for $1 < s_1 + s_2$ we can not obtain the estimate (3.2.1) for all rectangles Π since the certain neighborhoods of points with algebraic coordinates of small height and small degree do not contain any other points (α_1, α_2) with algebraic conjugate coordinates $\alpha_i \in \mathbb{A}_n(Q)$. This leads us to the definition of a set of small rectangles which are not affected by these 'anomalous' points.

Consider a square $\overline{\Pi} = I_1 \times I_2$ with $\lambda_1(I_1) = \lambda_1(I_2) = c_3 Q^{-s}$ where $\frac{1}{2} < s < \frac{3}{4}$. Given positive real numbers u_1, u_2 let us define the set $L_{u_1,u_2}(Q)$ of points $\mathbf{x} \in \mathbb{R}^2$ such that there exists a polynomial $P \in \mathcal{P}_2(Q)$ with leading coefficient b_2 satisfying the inequalities

$$\begin{cases} |P(x_i)| < h\, Q^{-u_i}, & i = 1, 2, \\ |b_2| < Q^{s - \frac{1}{2}}. \end{cases} \tag{3.2.2}$$

We say that the square $\overline{\Pi}$ is (u_1, u_2)- *ordinary* if $\overline{\Pi} \cap L_{u_1,u_2}(Q) = \emptyset$ and (u_1, u_2)-*special* otherwise.

For $\left(\frac{1}{2}, \frac{1}{2}\right)$-ordinary squares we can prove the estimate similar to (3.2.1).

Theorem 3.2.2. *For any $\left(\frac{1}{2}, \frac{1}{2}\right)$-ordinary square $\overline{\Pi} = I_1 \times I_2$ with middle point $\mathbf{d} = (d_1, d_2)$, $d_1 \neq d_2$ satisfying the following conditions:*

1. *$\lambda_1(I_i) = c_3 Q^{-s}$, where $\frac{1}{2} < s < \frac{3}{4}$;*
2. *$c_3 > c_0(n, \mathbf{d}) > 0$;*

any integer $n \geq 2$, and any real positive $Q > Q_0(n, \mathbf{d}, \mathbf{s})$ there exists a constant $c_4 = c_4(n, \mathbf{d}) > 0$, such that

$$\mathcal{N}_n^2(\mathbb{A}, Q, \overline{\Pi}) \geq c_4 Q^{n+1} \lambda_2\left(\overline{\Pi}\right).$$

The upper estimate is easier to prove and can be obtained for the bigger set of rectangles.

Theorem 3.2.3. *Let $\Pi = I_1 \times I_2$ be a rectangle with a middle point $\mathbf{d} = (d_1, d_2)$, $d_1 \neq d_2$ and $\lambda_1(I_i) = c_5 Q^{-s_i}$, $i = 1, 2$. Then for any $0 < s_1, s_2 < 1$, any integer $n \geq 2$, and any real positive $Q > Q_0(n, \mathbf{s}, \mathbf{d})$ we have*

$$\mathcal{N}_n^2(\mathbb{A}, Q, \Pi) < c_6 Q^{n+1} \lambda_2(\Pi),$$

where $c_6 = 2^{3n+9} n^2 \omega_n(3/2\, d_1) \omega_n(3/2\, d_2) |d_1 - d_2|^{-1}$.

3.2.1 Some Technical Lemmas

Before we start the proofs of Theorem 3.2.1, Theorem 3.2.2 and Theorem 3.2.3 let us formulate and prove some simple technical lemmas.

Lemma 3.2.4. *Let I be an interval with middle point d and length $\lambda_1(I) \ll Q^{-s}$, $s > 0$. Then for any polynomial $P \in \mathcal{P}_n(Q)$, any point $x \in I$, and any real positive $Q > Q_0(s, d)$ we have*

$$|P^{(k)}(x)| \leq \frac{n!}{(n-k)!} \omega_{n-k+1}(3/2\, d_i)\, Q.$$

Proof. Consider some point $x \in I$ and some polynomial $P(t) = \sum\limits_{k=0}^{n} a_k t^k \in \mathcal{P}_n(Q)$. We obtain

$$|P^{(k)}(x)| = \left| \sum_{j=0}^{n-k} \frac{(n-j)!}{(n-j-k)!} a_{n-j} x^{n-j-k} \right| \leq \frac{n!}{(n-k)!} Q \sum_{j=0}^{n-k} |x|^j.$$

Since $x \in I$ then for some $-1 \leq \theta \leq 1$ and $Q > Q_0$ we have

$$|x| = |d + \theta \lambda_1(I)| \leq |d| + \theta Q^{-s} \leq \frac{3}{2} |d|$$

and, hence,

$$|P^{(k)}(x)| \le \frac{n!}{(n-k)!}\omega_{n-k+1}(3/2\,d)\,Q.$$

□

Lemma 3.2.5. *Given some* $\mathbf{d}, \mathbf{K} \in \mathbb{R}^2$*, such that* $|d_1 - d_2| \neq 0$ *and* $K_1 \ge K_2 > 0$*, denote by* $G := G(\mathbf{d}, \mathbf{K})$ *a set of points* $\mathbf{b} \in \mathbb{Z}^2$ *satisfying*

$$|b_1 d_i + b_0| \le K_i, \quad i = 1, 2. \tag{3.2.3}$$

Then

$$\#G \le \left(4|d_1 - d_2|^{-1}K_1 + 1\right)(4K_2 + 1).$$

Proof. To avoid triviality assume that $G \neq \emptyset$ and choose some point $(b_1, b_0) \in G$. Assume that the following system of equations in two variables

$$b_1 d_i + b_0 = l_i, \quad i = 1, 2, \tag{3.2.4}$$

holds, where $|l_i| \le K_i$. Considering the difference of equations

$$b_1(d_1 - d_2) = l_1 - l_2,$$

we obtain

$$|b_1| \le (|l_1| + |l_2|)\,|d_1 - d_2|^{-1} \le 2|d_1 - d_2|^{-1}K_1.$$

This inequality implies that for all $(b_1, b_0) \in G$ the value b_1 belongs to the interval J_1, where

$$J_1 := \left(-2|d_1 - d_2|^{-1}K_1; 2|d_1 - d_2|^{-1}K_1\right).$$

Assume that for some fixed $b \in J_1$ there exist at least two points $\mathbf{b}_1, \mathbf{b}_2 \in G$ with $b_{1,1} = b_{2,1} = b$ and

$$bd_i + b_{j,0} = l_{i,j}, \quad i, j = 1, 2.$$

From these equalities it follows that

$$|b_{1,0} - b_{2,0}| = |l_{2,1} - l_{2,2}| \le 2K_2,$$

which implies that if at least one solution $(b, a) \in G$ exists, then for all $(b_1, b_0) \in G$ with $b_1 = b$ the value b_0 belongs to the interval $J_0(b)$, where

$$J_0(b) := (a - 2K_2; a + 2K_2).$$

Remembering that $b_1, b_0 \in \mathbb{Z}$, we conclude

$$\#G \le \left(4|d_1 - d_2|^{-1}K_1 + 1\right)(4K_2 + 1).$$

□

3.2.2 Proof of Theorem 3.2.1: Lower Bound

The main ingredient of the proof of Theorem 3.2.1 is the following lemma.

Lemma 3.2.6. *Consider some rectangle* $\Pi = I_1 \times I_2$ *with middle point* $\mathbf{d} = (d_1, d_2)$, $d_1 \neq d_2$ *satisfying the conditions:*

1. $\lambda_1(I_i) = c_{1,i} Q^{-s_i}$ *where* $s_i < 1$ *and* $0 < s_1 + s_2 \leq 1$, $i = 1, 2$;
2. $c_{1,1} c_{1,2} > c_0(n, \mathbf{d}) > 0$ *for* $s_1 + s_2 = 1$.

Given a vector $\mathbf{v} = (v_1, v_2) \in \mathbb{R}_+^2$ *with* $v_1 + v_2 = n-1$ *denote by* $L := L(Q, \delta_n, \kappa, \mathbf{v}, \Pi)$ *the set of points* $\mathbf{x} \in \Pi$ *such that there exists a polynomial* $P \in \mathcal{P}_n(Q)$ *satisfying the inequalities*

$$\begin{cases} |P(x_i)| < h_n Q^{-v_i}, \\ \min\limits_i \{|P'(x_i)|\} < \delta_n Q, \quad i = 1, 2. \end{cases} \tag{3.2.5}$$

Then for any $0 < \kappa < 1$, *any* $0 < \delta_n \leq \delta_0(n, \mathbf{d}, \kappa)$, *and any real positive* $Q > Q_0(n, \mathbf{s}, \mathbf{v}, \mathbf{d}, \kappa)$ *we have*

$$\lambda_2(L) < \kappa \lambda_2(\Pi).$$

Proof. Since $d_1 \neq d_2$ we can assume that for every point $\mathbf{x} \in \Pi$ and for $Q > Q_0$ the following holds

$$|x_1 - x_2| > \varepsilon = \tfrac{|d_1 - d_2|}{2}. \tag{3.2.6}$$

Let us introduce some additional notation. Given a polynomial P of degree n let $\mathcal{A}(P) := \{\alpha_i, 1 \leq i \leq n\}$ be the set of roots of P and let

$$S(\alpha_i) := \left\{ x \in \mathbb{R} : |x - \alpha_i| = \min_{1 \leq j \leq n} |x - \alpha_j| \right\}.$$

Denote by

- L_1 the set of points $\mathbf{x} \in \Pi$ such that there exists an irreducible polynomial $P \in \mathcal{P}_n(Q)$ satisfying inequalities (3.2.5) and the condition $|P'(x_1)| < \delta_n Q$;
- L_2 the set of points $\mathbf{x} \in \Pi$ such that there exists an irreducible polynomial $P \in \mathcal{P}_n(Q)$ satisfying inequalities (3.2.5) and the condition $|P'(x_2)| < \delta_n Q$;
- L_3 the set of points $\mathbf{x} \in \Pi$ such that there exists a reducible polynomial $P \in \mathcal{P}_n(Q)$ satisfying inequalities (3.2.5).

Clearly, we have $L \subset (L_1 \cup L_2 \cup L_3)$.

The biggest part of the proof is devoted to the case of irreducible polynomials. We will start by considering this case and deriving the estimates for $\lambda_1(L_1)$ and $\lambda_1(L_2)$. Without loss of generality, assume that $|P'(x_1)| < \delta_n Q$ and consider the set L_1.

In this case the main idea is to split the interval T_i, which contains all possible values of $|P'(x_i)|$ for $\mathbf{x} \in \Pi$, into sub-intervals $T_{i,1}$, $T_{i,2}$, $T_{i,3}$ and consider the cases

$|P'(x_i)| \in T_{i,k}$, $k = 1, 2, 3$ separately. This splitting is performed as follows

$$T_{i,1} = \left[0; \quad 2c_7\, Q^{\frac{1}{2}-\frac{v_i}{2}}\right), \quad T_{i,2} = \left[2c_7\, Q^{\frac{1}{2}-\frac{v_i}{2}}; \quad Q^{\frac{1}{2}-\frac{v_i}{2}+\frac{v_i}{2(n-1)}}\right), \quad i = 1, 2;$$

$$T_{1,3} = \left[Q^{\frac{1}{2}-\frac{v_1}{2}+\frac{v_1}{2(n-1)}}; \quad \delta_n\, Q\right), \qquad T_{2,3} = \left[Q^{\frac{1}{2}-\frac{v_2}{2}+\frac{v_2}{2(n-1)}}; \quad n\omega_n(3/2\, d_2)\, Q\right).$$

Without loss of generality, we will assume that $|d_1| < |d_2|$. We would like to verify that if a polynomial $P \in \mathcal{P}_n(Q)$ satisfies the inequalities

$$|P'(x_i)| \geq 2c_7\, Q^{\frac{1}{2}-\frac{v_i}{2}}, \tag{3.2.7}$$

where $\mathbf{x} \in \Pi$ and $c_7 = 2^{n-1}n \max(h_n, 1) \max(1, \omega_{n-1}(d_2))$ then

$$\tfrac{1}{2}|P'(x_i)| \leq |P'(\alpha_i)| \leq 2|P'(x_i)|, \quad i = 1, 2,$$

where $x_i \in S(\alpha_i)$. Let us write a Taylor expansion of the polynomial P' at point x_i

$$P'(x_i) = P'(\alpha_i) + P''(\alpha_i)(x_i - \alpha_i) + \ldots + \tfrac{1}{(n-1)!}P^{(n)}(\alpha_i)(x_i - \alpha_i)^{n-1}. \tag{3.2.8}$$

Using Lemma A.1.14 and the estimates (3.2.5) for $Q > Q_0$, we have

$$|x_i - \alpha_i| \leq nh_n c_7^{-1}\, Q^{-\frac{v_i+1}{2}} < Q^{-\frac{v_i+1}{2}}.$$

Then, for $s_i > 0$ and $Q > Q_0$ we get

$$|x_i| \leq |d_i| + \tfrac{1}{2}\lambda_1(I_i) \leq |d_i| + \tfrac{1}{4}|d_i| = \tfrac{5}{4}|d_i|$$

and, thus,

$$|\alpha_i| \leq |x_i| + Q^{-\frac{v_i+1}{2}} < \tfrac{5}{4}|d_i| + \tfrac{1}{4}|d_i| = \tfrac{3}{2}|d_i|.$$

From this estimate and Lemma 3.2.4 we obtain the following inequality for every term in Taylor expansion (3.2.8) starting from the second one

$$\begin{aligned}\left|\tfrac{1}{(k-1)!}P^{(k)}(\alpha_i)(x_i - \alpha_i)^{k-1}\right| &< \tbinom{k-1}{n-1}\, n\omega_{n-k+1}(3/2\, d_2)\, Q^{1-\frac{(k-1)(1+v_i)}{2}} \\ &\leq \tbinom{k-1}{n-1}\, n\omega_{n-1}(3/2\, d_2)\, Q^{\frac{1}{2}-\frac{v_i}{2}}.\end{aligned}$$

Finally, we get the following estimate

$$\begin{aligned}&\left|P''(\alpha_i)(x_i - \alpha_i) + \ldots + \tfrac{1}{(n-1)!}P^{(n)}(\alpha_i)(x_i - \alpha_i)^{n-1}\right| \\ &\qquad < 2^{n-1}n\omega_{n-1}(3/2\, d_2)\, Q^{\frac{1}{2}-\frac{v_i}{2}} < \tfrac{1}{2}|P'(x_i)|,\end{aligned}$$

and, by substituting this inequality to (3.2.8) we obtain

$$\tfrac{1}{2}|P'(x_i)| \leq |P'(\alpha_i)| \leq 2|P'(x_i)|.$$

This means that for $|P'(x_i)| \in T_{i,3}$ and $|P'(x_i)| \in T_{i,2}$ we have $|P'(\alpha_i)| \in \overline{T}_{i,3}$ and $|P'(\alpha_i)| \in \overline{T}_{i,2}$ respectively, where

$$\overline{T}_{1,3} = \left[\tfrac{1}{2}\, Q^{\frac{1}{2}-\frac{v_1}{2}+\frac{v_1}{2(n-1)}}; \quad 2\delta_n\, Q\right), \qquad \overline{T}_{2,3} = \left[\tfrac{1}{2}\, Q^{\frac{1}{2}-\frac{v_2}{2}+\frac{v_2}{2(n-1)}}; \quad 2n\omega_n(3/2\, d_2)\, Q\right),$$

$$\overline{T}_{i,2} = \left[c_7\, Q^{\frac{1}{2}-\frac{v_i}{2}}; \quad 2\, Q^{\frac{1}{2}-\frac{v_i}{2}+\frac{v_i}{2(n-1)}}\right), \quad i = 1, 2.$$

Now we are going to consider the following cases:

- the case of polynomials of the second degree $n = 2$ (see Subsection 3.2.2.1);
- the case of irreducible polynomials:

  $|P'(\alpha_1)| \in \overline{T}_{1,3}$, $|P'(\alpha_2)| \in \overline{T}_{2,3}$ (see Subsection 3.2.2.2);

  $|P'(\alpha_1)| \in \overline{T}_{1,2}$, $|P'(\alpha_2)| \in \overline{T}_{2,2}$ (see Subsection 3.2.2.3);

  $|P'(x_1)| \in T_{1,1}$, $|P'(x_2)| \in T_{2,1}$ (see Subsection 3.2.2.4);

  $|P'(\alpha_1)| \in \overline{T}_{1,3}$, $|P'(\alpha_2)| \in \overline{T}_{2,2}$ or $|P'(\alpha_1)| \in \overline{T}_{1,2}$, $|P'(\alpha_2)| \in \overline{T}_{2,3}$ (see Subsection 3.2.2.5);

  $|P'(\alpha_1)| \in \overline{T}_{1,3}$, $|P'(x_2)| \in T_{2,1}$ or $|P'(x_1)| \in T_{1,1}$, $|P'(\alpha_2)| \in \overline{T}_{2,3}$ (see Subsection 3.2.2.5);

  $|P'(\alpha_1)| \in \overline{T}_{1,2}$, $|P'(x_2)| \in T_{2,1}$ or $|P'(x_1)| \in T_{1,1}$, $|P'(\alpha_2)| \in \overline{T}_{2,2}$ (see Subsection 3.2.2.5);
- the case of reducible polynomials (see Subsection 3.2.2.6).

Considering some of the cases above, we are going to use induction on the degree n. Let us first consider the system (3.2.5) for polynomials of the second degree, which will provide us the base of induction.

3.2.2.1 The base of induction: polynomials of the second degree.

Consider the system (3.2.5) for $n = 2$. Given some real numbers $\gamma_{2,1}, \gamma_{2,2} > 0$ under condition $\gamma_{2,1} + \gamma_{2,2} = 1$ denote by $L' := L_2(Q, \delta_2, \kappa, \boldsymbol{\gamma}_2, \Pi)$ the set of points $\mathbf{x} \in \Pi$ such that there exists a polynomial $P \in \mathcal{P}_2(Q)$ satisfying the inequalities

$$\begin{cases} |P(x_i)| < h_2\, Q^{-\gamma_{2,i}}, \\ \min\limits_i \{|P'(x_i)|\} < \delta_2\, Q, \quad i = 1, 2. \end{cases} \tag{3.2.9}$$

We will show that for all rectangles Π satisfying the conditions of Lemma 3.2.6, for any $\delta_2 < \delta_0(\mathbf{d}, \mathbf{s}, \kappa)$, and any $Q > Q_0(\mathbf{s}, \boldsymbol{\gamma}_2, \mathbf{d}, \kappa)$ we have

$$\lambda_2\left(L'\right) < \kappa\, \lambda_2\left(\Pi\right).$$

It should be mentioned that if polynomial $P(t) = b_1 t - b_0$ is linear, then we apply Lemma A.1.14 to obtain

$$\left|x_i - \tfrac{b_0}{b_1}\right| \ll Q^{-\gamma_{2,i}} < \tfrac{\varepsilon}{4}, \quad i = 1, 2$$

for $Q > Q_0$. Hence, we immediately have $|x_1 - x_2| < \varepsilon$ which contradicts to (3.2.6). Thus, $\deg P = 2$.

Consider the polynomial $P(t) = b_2 t^2 + b_1 t + b_0 \in \mathcal{P}_2(Q)$ with roots α_1 and α_2. We would like to estimate the value $|b_2|$ assuming that P satisfies (3.2.9). Let us start

with estimating the values $|P'(\alpha_1)|$ and $|P'(\alpha_2)|$. By the third inequality of Lemma A.1.14, for every polynomial P satisfying (3.2.9) at a point $\mathbf{x} \in \Pi$, we have

$$|x_i - \alpha_i| < \left(|P(x_i)||b_2|^{-1}\right)^{1/2} < h_2^{1/2} Q^{-\frac{\gamma_{2,i}}{2}} < \tfrac{\varepsilon}{8}, \tag{3.2.10}$$

for $Q > Q_0$ and $x_i \in S(\alpha_i)$.

From (3.2.10) and (3.2.6) we obtain

$$|\alpha_1 - \alpha_2| > |x_1 - x_2| - |x_1 - \alpha_1| - |x_2 - \alpha_2| > \tfrac{3}{4}\,\varepsilon$$

and

$$|\alpha_1 - \alpha_2| < |x_1| + |x_2| + |x_1 - \alpha_1| + |x_2 - \alpha_2| < |d_1| + |d_2| + 1 + \tfrac{\varepsilon}{4}.$$

This leads to the following bounds

$$|P'(\alpha_i)| = |b_2|\,|\alpha_1 - \alpha_2| > \tfrac{3}{4}\,\varepsilon\,|b_2|. \tag{3.2.11}$$

The inequalities (3.2.10) also yield the estimates

$$|P'(x_i)| \le |b_2|\,(|\alpha_1 - x_i| + |\alpha_2 - x_i|) \le \left(|d_2| + 1 + \tfrac{\varepsilon}{4}\right)\,|b_2|. \tag{3.2.12}$$

Now upper bounds for $|P'(\alpha_i)|$ can be obtained from the Taylor expansion of the polynomial P'

$$|P'(\alpha_i)| \le |P'(x_i)| + |P''(x_i)|\,|x_i - \alpha_i| \le |P'(x_i)| + \tfrac{\varepsilon}{2}\,|b_2|. \tag{3.2.13}$$

Finally, the estimates (3.2.11) and (3.2.13) lead to the inequality

$$|b_2| < 4\varepsilon^{-1} \min_i \left\{|P'(x_i)|\right\} < 4\delta_2\varepsilon^{-1}Q. \tag{3.2.14}$$

From Lemma A.1.14 and the estimates (3.2.11) it follows that the set L' is contained in a union $\bigcup\limits_{P\in\mathcal{P}_2(Q)} \sigma_P$, where

$$\sigma_P := \left\{\mathbf{x} \in \Pi : \quad |x_i - \alpha_i| < 2h_2\varepsilon^{-1}\,Q^{-\gamma_{2,i}}|b_2|^{-1}, i = 1, 2\right\}.$$

Simple calculations show that for $c_{1,1}c_{1,2} > 2^4\kappa^{-1}h_2^2\varepsilon^{-2}$ the measure of the set σ_P is much smaller than the measure of the rectangle Π

$$\lambda_2\left(\sigma_P\right) \le 2^4 h_2^2\varepsilon^{-2}Q^{-1}|b_2|^{-2} < \kappa\,c_{1,1}c_{1,2}\,Q^{-1} = \kappa\,\lambda_2\left(\Pi\right).$$

Let us estimate the measure of the set L'

$$\lambda_2\left(L'\right) \le \sum_{P\in\mathcal{P}_2(Q)} \lambda_2\left(\sigma_P\right) \le 2^4 h_2^2\varepsilon^{-2}Q^{-1} \sum_{\substack{b_2,b_1,b_0\le Q:\\ P(t)=b_2t^2+b_1t+b_0,\\ \sigma_P\neq\emptyset}} |b_2|^{-2}. \tag{3.2.15}$$

We need to estimate the number of polynomials $P \in \mathcal{P}_2(Q)$ with fixed leading coefficient such that the system (3.2.9) holds for some point $\mathbf{x} \in \Pi$.

Assume that the inequalities (3.2.9) hold for the polynomial P and the point $\mathbf{x}_0 \in \Pi$. Let us estimate the value of the polynomial P at points d_i. From the Taylor expansion of polynomial P we have

$$\begin{aligned}|P(d_i)| &= |P(x_{0,i}) + P'(x_{0,i})(x_{0,i} - d_i) + \tfrac{1}{2}P''(x_{0,i})(x_{0,i} - d_i)^2| \\ &\leq |P(x_{0,i})| + |P'(x_{0,i})|\lambda_1(I_i) + |b_2|\left(\lambda_1(I_i)\right)^2.\end{aligned}$$

Thus, from (3.2.12) for $Q > Q_0$ we obtain

$$|P(d_i)| < |P(x_{0,i})| + c_8|b_2|\lambda_1(I_i) \leq 2c_8 \max\left(1, |b_2|\lambda_1(I_i)\right),$$

where $c_8 > 1$. Without loss of generality we assume that $\lambda_1(I_1) \leq \lambda_1(I_2)$.

Consider the system of equations

$$\begin{cases} b_2 d_1^2 + b_1 d_1 + b_0 = l_1, \\ b_2 d_2^2 + b_1 d_2 + b_0 = l_2 \end{cases} \tag{3.2.16}$$

in three variables $b_2, b_1, b_0 \in \mathbb{Z}$, where $|l_i| \leq 2c_8 \max\left(1, |b_2|\lambda_1(I_i)\right)$.

Let us estimate the number of possible solutions of (3.2.16) for a fixed b_2. Assume that for chosen b_2 there exists at least one solution $(b_2, b_{1,1}, b_{1,0})$ and consider the system of linear equations (3.2.16) for two different triples $(b_2, b_{1,1}, b_{1,0})$ and $(b_2, b_{2,1}, b_{2,0})$:

$$b_2 d_i^2 + b_{j,1} d_i + b_{j,0} = l_{j,i}, \quad i, j = 1, 2.$$

Simple transformations lead to the following system of equations in two variables $\tilde{b}_1 = b_{1,1} - b_{2,1}$ and $\tilde{b}_0 = b_{1,0} - b_{2,0}$:

$$\begin{cases} \tilde{b}_1 d_1 + \tilde{b}_0 = l_{1,1} - l_{2,1}, \\ \tilde{b}_1 d_2 + \tilde{b}_0 = l_{1,2} - l_{2,2}. \end{cases} \tag{3.2.17}$$

Since $|l_{1,i} - l_{2,i}| \leq 4c_8 \max\left(1, |b_2|\lambda_1(I_i)\right)$ and $|d_1 - d_2| = 2\varepsilon > 0$ then applying Lemma 3.2.5 with $K_i = 4c_8 \max\left(1, |b_2|\lambda_1(I_i)\right)$ we conclude

$$\begin{aligned}\#(\tilde{b}_1, \tilde{b}_0) &\leq \left(2^4 c_8 \varepsilon^{-1} \max\left(1, |b_2|\lambda_1(I_1)\right) + 1\right)\left(2^4 c_8 \max\left(1, |b_2|\lambda_1(I_i)\right) + 1\right) \\ &\leq 2^{10} c_8^2 \varepsilon^{-1} \max\left(1, |b_2|\lambda_1(I_1)\right) \max\left(1, |b_2|\lambda_1(I_i)\right).\end{aligned}$$

Thus, for a fixed value of the coefficient b_2 we get following estimate

$$\#(b_1, b_0) \leq \begin{cases} 2^{10}\varepsilon^{-1} c_8^2 |b_2|^2 \lambda_2(\Pi), & |b_2| \geq \frac{1}{\lambda_1(I_1)}, \\ 2^{10}\varepsilon^{-1} c_8^2 |b_2| \lambda_1(I_2), & \frac{1}{\lambda_1(I_2)} \leq |b_2| < \frac{1}{\lambda_1(I_1)}, \\ 2^{10}\varepsilon^{-1} c_8^2, & |b_2| < \frac{1}{\lambda_1(I_2)}. \end{cases} \tag{3.2.18}$$

According to (3.2.18) we need to consider the following cases.

Case 1: $\frac{1}{\lambda_1(I_1)} \leq |b_2| \leq 4\delta_2 \varepsilon^{-1} Q$.

In this case the first estimate of (3.2.18) holds and for $\delta_2 < 2^{-18}\kappa^{-1}\varepsilon^4 c_8^{-2} h_2^{-2}$ we have

$$\lambda_2\left(L'\right) \le 2^{14}\varepsilon^{-3} c_8^2 h_2^2\, Q^{-1}\lambda_2\left(\Pi\right)\cdot 4\delta_2\varepsilon^{-1}\, Q < \tfrac{\kappa}{3}\,\lambda_2\left(\Pi\right).$$

Case 2: $\frac{1}{\lambda_1(I_2)} \le |b_2| < \frac{1}{\lambda_1(I_1)}$.

The second estimate of (3.2.18) holds and we get

$$\lambda_2\left(L'\right) \ll Q^{-1}\lambda_1\left(I_2\right) \sum_{(\lambda_1(I_2))^{-1}\le|b_2|\le(\lambda_1(I_1))^{-1}} |b_2|^{-1} \ll Q^{-1}\ln Q\,\lambda_1\left(I_2\right).$$

Hence, for $\varepsilon_1 = \frac{1-s_1}{2}$ and $Q > Q_0$ we obtain

$$\lambda_2\left(L'\right) \ll Q^{-1+\varepsilon_1}\lambda_1\left(I_2\right) \ll Q^{-\varepsilon_1}\lambda_2\left(\Pi\right) \le \tfrac{\kappa}{3}\,\lambda_2\left(\Pi\right).$$

Case 3: $1 \le |b_2| < \frac{1}{\lambda_1(I_2)}$.

In this case the third estimate of (3.2.18) leads to

$$\lambda_2\left(L'\right) \le 2^{14}\varepsilon^{-3} c_8^2 h_2^2\, Q^{-1} \sum_{1\le|b_2|\le(\lambda_1(I_2))^{-1}} |b_2|^{-2} \le \tfrac{\kappa}{3}\,\lambda_2\left(\Pi\right),$$

for $c_{1,1}c_{1,2} > 2^{17}\kappa^{-1}\pi^2 c_8^2\varepsilon^{-3}h_2^2$.

Combining these estimates with (3.2.15) finishes the proof.

3.2.2.2 The induction step: reducing the degree of the polynomial.

In this subsection we consider the case $|P'(\alpha_i)| \in \overline{T}_{i,3}$, $i = 1, 2$ where we have the following system of inequalities

$$\begin{cases} |P(x_i)| < h_n\, Q^{-v_i}, \quad i = 1, 2, \\ \frac{1}{2}\, Q^{\frac{1}{2}-\frac{v_1}{2}+\frac{v_1}{2(n-1)}} \le |P'(\alpha_1)| < 2\delta_n\, Q, \\ \frac{1}{2}\, Q^{\frac{1}{2}-\frac{v_2}{2}+\frac{v_2}{2(n-1)}} \le |P'(\alpha_2)| < 2n\omega_n(3/2\, d_2)\, Q. \end{cases} \tag{3.2.19}$$

Denote by $L_{3,3}$ the set of points $\mathbf{x} \in \Pi$ such that the inequalities (3.2.19) hold for some polynomial $P \in \mathcal{P}_n(Q)$. By Lemma A.1.14, it follows that

$$L_{3,3} \subset \bigcup_{P\in\mathcal{P}_n(Q)} \bigcup_{\boldsymbol{\alpha}\in\mathcal{A}^2(P)} \sigma_P(\boldsymbol{\alpha}),$$

where

$$\sigma_P(\boldsymbol{\alpha}) := \left\{\mathbf{x} \in \Pi : \quad |x_i - \alpha_i| < 2^{n-1} h_n\, Q^{-v_i}\, |P'(\alpha_i)|^{-1}, i = 1, 2\right\}, \tag{3.2.20}$$

which implies that the following estimate for $\lambda_2\left(L_{3,3}\right)$ holds

$$\lambda_2\left(L_{3,3}\right) \le \sum_{P\in\mathcal{P}_n(Q)} \sum_{\boldsymbol{\alpha}\in\mathcal{A}^2(P)} \lambda_2\left(\sigma_P(\boldsymbol{\alpha})\right).$$

Together with the sets $\sigma_P(\boldsymbol{\alpha})$ consider the following expanded sets

$$\begin{aligned}\sigma'_P(\boldsymbol{\alpha}) :&= \sigma'_{P,1}(\alpha_1) \times \sigma'_{P,2}(\alpha_2)\\ &= \left\{\mathbf{x} \in \Pi : \quad |x_i - \alpha_i| < c_9\, Q^{-\gamma_{n-1,i}}\, |P'(\alpha_i)|^{-1}, i = 1, 2\right\}, \end{aligned} \tag{3.2.21}$$

where $\gamma_{n-1,i} := \frac{(n-2)v_i}{n-1}$. Simple calculations show that for $Q > Q_0$ and $n \geq 2$ the measure of the set $\sigma'_P(\boldsymbol{\alpha})$ is much smaller than the measure of the rectangle Π

$$\lambda_2\left(\sigma'_P(\boldsymbol{\alpha})\right) \leq 4c_9^2\, Q^{-n+2} Q^{-1+\frac{n-2}{2}} < 4c_9^2\, Q^{-\frac{n}{2}} < \lambda_2\left(\Pi\right).$$

Using (3.2.20) and (3.2.21) it is easy to see that the measures $\lambda_2\left(\sigma_P(\boldsymbol{\alpha})\right)$ and $\lambda_2\left(\sigma'_P(\boldsymbol{\alpha})\right)$ are related as follows

$$\lambda_2\left(\sigma_P(\boldsymbol{\alpha})\right) \leq 2^{2n-2} h_n^2 c_9^{-2}\, Q^{-1} \lambda_2\left(\sigma'_P(\boldsymbol{\alpha})\right). \tag{3.2.22}$$

Given a fixed $a \in \mathbb{Z}$ let $\mathcal{P}_n(Q, a) \subset \mathcal{P}_n(Q)$ denote a subclass of polynomials with the leading coefficient equal to a

$$\mathcal{P}_n(Q, a) := \{P \in \mathcal{P}_n(Q) : P(t) = at^n + \ldots + a_0\}.$$

Since $-Q \leq a \leq Q$, the number of subclasses $\mathcal{P}_n(Q, a)$ is

$$\#\{a\} = 2Q + 1. \tag{3.2.23}$$

We are going to apply Sprindžuk's method of essential and non-essential sets [62]. Consider a family of sets $\sigma'_P(\boldsymbol{\alpha})$, $P \in \mathcal{P}_n(Q, a)$. A set $\sigma'_{P_1}(\boldsymbol{\alpha}_1)$ is called *essential* if for every $\sigma'_{P_2}(\boldsymbol{\alpha}_2)$, $P_2 \neq P_1$, the following holds

$$\lambda_2\left(\sigma'_{P_1}(\boldsymbol{\alpha}_1) \cap \sigma'_{P_2}(\boldsymbol{\alpha}_2)\right) < \tfrac{1}{2}\lambda_2\left(\sigma'_{P_1}(\boldsymbol{\alpha}_1)\right). \tag{3.2.24}$$

Otherwise, the set $\sigma'_{P_1}(\boldsymbol{\alpha}_1)$ is called *non-essential*.

The case of essential sets. It is easy to ensure, that for any $-Q \leq a \leq Q$, we have the following estimate

$$\sum_{P \in \mathcal{P}_n(Q,a)} \sum_{\substack{\boldsymbol{\alpha} \in \mathcal{A}^2(P):\\ \sigma'_P(\boldsymbol{\alpha})\text{—essential}}} \lambda_2\left(\sigma'_P(\boldsymbol{\alpha})\right) \leq 4\,\lambda_2\left(\Pi\right). \tag{3.2.25}$$

Then from (3.2.22) with $c_9 = 2^{n+4}\kappa^{-1/2}h_n$, (3.2.23), and (3.2.25) we get

$$\begin{aligned}\sum_a \sum_{P \in \mathcal{P}_n(Q,a)} \sum_{\substack{\boldsymbol{\alpha} \in \mathcal{A}^2(P):\\ \sigma'_P(\boldsymbol{\alpha})\text{—ess.}}} \lambda_2\left(\sigma_P(\boldsymbol{\alpha})\right) &\leq 2^{-10} \sum_{P \in \mathcal{P}_n(Q,a)} \sum_{\substack{\boldsymbol{\alpha} \in \mathcal{A}^2(P):\\ \sigma'_P(\boldsymbol{\alpha})\text{—ess.}}} \lambda_2\left(\sigma'_P(\boldsymbol{\alpha})\right)\\ &< \tfrac{\kappa}{72}\,\lambda_2\left(\Pi\right). \end{aligned} \tag{3.2.26}$$

The case of non-essential sets. If a set $\sigma'_{P_1}(\boldsymbol{\alpha}_1)$ is non-essential, then there exists a set $\sigma'_{P_2}(\boldsymbol{\alpha}_2)$ such that $\lambda_2\left(\sigma'_{P_1}(\boldsymbol{\alpha}_1) \cap \sigma'_{P_2}(\boldsymbol{\alpha}_2)\right) > \frac{1}{2}\lambda_2\left(\sigma'_{P_1}(\boldsymbol{\alpha}_1)\right)$. Consider the

polynomial $R = P_2 - P_1$, $\deg R \le n-1$, $H(R) \le 2Q$. Let us estimate the value of polynomials R and R' at points $\mathbf{x} \in \big(\sigma'_{P_1}(\boldsymbol{\alpha}_1) \cap \sigma'_{P_2}(\boldsymbol{\alpha}_2)\big)$.

Consider the Taylor expansions of the polynomials P_1 and P_2 in the interval $\sigma'_{P_1,i}(\alpha_{1,i}) \cap \sigma'_{P_2,i}(\alpha_{2,i})$

$$P_j(x_i) = P'_j(\alpha_{j,i})(x_i - \alpha_{j,i}) + \ldots + \tfrac{1}{n!}\, P_j^{(n)}(\alpha_{j,i})(x_i - \alpha_{j,i})^n. \tag{3.2.27}$$

From the estimate (3.2.19), (3.2.21), and Lemma 3.2.4 we have

$$|P'_j(\alpha_{j,i})(x_i - \alpha_{j,i})| \le c_9\, Q^{-\gamma_{n-1,i}},$$

and, for $k \ge 2$, we get

$$\begin{aligned}\left|\tfrac{1}{k!} P_j^{(k)}(\alpha_{j,i})(x_i - \alpha_{j,i})^k\right| &\le \tbinom{k}{n}\, \omega_{n-k+1}(3/2\, d_i) c_9^k\, Q^{1-k\gamma_{n-1,i}-\frac{k}{2}+\frac{k}{2}\gamma_{n-1,i}} \\ &\le \tbinom{k}{n}\, \omega_{n-1}(3/2\, d_i) c_9^k\, Q^{-\gamma_{n-1,i}}.\end{aligned}$$

Substituting these estimates into (3.2.27) we obtain

$$|P_j(x_i)| \le \omega_{n-1}(3/2\, d_2)(1 + c_9)^n\, Q^{-\gamma_{n-1,i}},$$

and, thus,

$$|R(x_i)| < |P_1(x_i)| + |P_2(x_i)| < 2\omega_{n-1}(3/2\, d_2)(1 + c_9)^n\, Q^{-\gamma_{n-1,i}} \tag{3.2.28}$$

Analogously, consider Taylor expansions of the polynomials P'_1 and P'_2 in the interval $\sigma'_{P_1,i}(\alpha_{1,i}) \cap \sigma'_{P_2,i}(\alpha_{2,i})$

$$P'_j(x_i) = P'_j(\alpha_{j,i}) + \ldots + \tfrac{1}{(n-1)!} P_j^{(n)}(\alpha_{j,i})(x_i - \alpha_{j,i})^{n-1}, \tag{3.2.29}$$

and, from the estimate (3.2.19), (3.2.21), and Lemma 3.2.4 we obtain

$$\begin{aligned}\left|\tfrac{1}{(k-1)!} P_j^{(k)}(\alpha_i)(x_i - \alpha_i)^{k-1}\right| &\le n\tbinom{k-1}{n-1}\, \omega_{n-k+1}(3/2\, d_2) c_9^{k-1}\, Q^{1-(k-1)\left(\frac{\gamma_{n-1,i}}{2}+\frac{1}{2}\right)} \\ &\le n\tbinom{k-1}{n-1}\, \omega_{n-1}(3/2\, d_2) c_9^{k-1}\, |P'_j(\alpha_i)|,\end{aligned}$$

for $k \ge 2$. Substituting these estimates into (3.2.27) we have

$$|P_j(x_i)| \le n\omega_{n-1}(3/2\, d_2)(1 + c_9)^{n-1}\, |P'_j(\alpha_{j,i})|$$

and, thus, from (3.2.19) we finally get

$$\begin{aligned}\min_i \big\{|R'(x_i)|\big\} &\le \min_i \big\{|P'_1(x_i)|\big\} + \min_i \big\{|P'_2(x_i)|\big\} \\ &\le 4n\omega_n(3/2\, d_2)(1 + c_9)^{n-1}\delta_n\, Q.\end{aligned} \tag{3.2.30}$$

The inequalities (3.2.28) and (3.2.30) hold for every point $\mathbf{x} \in \big(\sigma'_{P_1}(\boldsymbol{\alpha}_1) \cap \sigma'_{P_2}(\boldsymbol{\alpha}_2)\big)$. Applying Lemma A.1.15 with the fact $\lambda_1\Big(\sigma'_{P_1,i}(\alpha_{1,i}) \cap \sigma'_{P_2,i}(\alpha_{2,i})\Big) > \frac{1}{2}\lambda_1\Big(\sigma'_{P_1,i}(\alpha_{1,i})\Big)$ we obtain that for every point $\mathbf{x} \in \sigma'_{P_1}(\boldsymbol{\alpha}_1)$ the following

$$|R(x_i)| < c_{10}\, Q^{-\gamma_{n-1,i}}, \quad \min_i \big\{|R'(x_i)|\big\} < c_{11}\delta_n\, Q \tag{3.2.31}$$

holds for some c_{10} and c_{11} depending on n and $\mathbf{d}$.

Denote by L' the set of points $\mathbf{x} \in \Pi$ such that there exists a polynomial $R \in \mathcal{P}_{n-1}(Q_1)$ satisfying the inequalities

$$\begin{cases} |R(x_i)| < c_{12} h_{n-1}\, Q_1^{-\gamma_{n-1,i}}, \quad i = 1,2 \\ \min\limits_i \{|R'(x_i)|\} < \delta_{n-1}\, Q_1, \end{cases}$$

where $Q_1 = 2Q$, $c_{12} = \max\limits_i (2^{\gamma_{n-1,i}})\, c_{10} h_{n-1}^{-1}$ and $\delta_{n-1} = 2c_{11}\, \delta_n$.

The estimates (3.2.31) imply that for any $-Q \le a \le Q$ we have

$$\bigcup_{P \in \mathcal{P}_n(Q,a)} \bigcup_{\substack{\boldsymbol{\alpha} \in \mathcal{A}^2(P): \\ \sigma'_P(\boldsymbol{\alpha}) \text{—non-essential}}} \sigma'_P(\boldsymbol{\alpha}) \subset L'.$$

Thus, by the induction hypothesis we obtain

$$\sum_a \sum_{P \in \mathcal{P}_n(Q,a)} \sum_{\substack{\boldsymbol{\alpha} \in \mathcal{A}^2(P): \\ \sigma'_P(\boldsymbol{\alpha}) \text{—non-essential}}} \lambda_2\left(\sigma_P(\boldsymbol{\alpha})\right) \le \lambda_2\left(L'\right) \le \tfrac{\kappa}{72}\, \lambda_2\left(\Pi\right), \tag{3.2.32}$$

for a sufficiently small δ_n and $Q > Q_0$. Then, the estimates (3.2.26) and (3.2.32) allow us to write

$$\lambda_2\left(L_{3,3}\right) \le \tfrac{\kappa}{36}\, \lambda_2\left(\Pi\right).$$

3.2.2.3 The case of sub-intervals $\bar{T}_{1,2}$ and $\bar{T}_{2,2}$

For $|P'(\alpha_1)| \in \bar{T}_{1,2}$ and $|P'(\alpha_2)| \in \bar{T}_{2,2}$ we have the following system of inequalities

$$\begin{cases} |P(x_i)| < h_n\, Q^{-v_i}, \\ c_7\, Q^{\frac{1}{2} - \frac{v_i}{2}} \le |P'(\alpha_i)| < 2Q^{\frac{1}{2} - \frac{v_i}{2} + \frac{v_i}{2(n-1)}}, \quad i = 1,2. \end{cases} \tag{3.2.33}$$

Denote by $L_{2,2}$ the set of points $\mathbf{x} \in \Pi$ such that there exists a polynomial $P \in \mathcal{P}_n(Q)$ satisfying (3.2.33). By Lemma A.1.14 we get

$$L_{2,2} \subset \bigcup_{P \in \mathcal{P}_n(Q)} \bigcup_{\boldsymbol{\alpha} \in \mathcal{A}^2(P)} \sigma_P(\boldsymbol{\alpha}),$$

where

$$\sigma_P(\boldsymbol{\alpha}) := \left\{ \mathbf{x} \in \Pi : \quad |x_i - \alpha_i| \le 2^{n-1} h_n c_7^{-1}\, Q^{-\frac{v_i+1}{2}}, i = 1,2 \right\}. \tag{3.2.34}$$

This leads to the following estimate

$$\lambda_2\left(L_{2,2}\right) \le \sum_{P \in \mathcal{P}_n(Q)} \sum_{\boldsymbol{\alpha} \in \mathcal{A}^2(P)} \lambda_2\left(\sigma_P(\boldsymbol{\alpha})\right).$$

In this case we can not apply induction since the degree of the polynomial can not be reduced. Let us use a different method to estimate the measure of the set $L_{2,2}$.

Let us cover the rectangle Π by a set of disjoint rectangles $\Pi_k = J_{1,k} \times J_{2,k}$, where $\lambda_1(J_{i,k}) = \frac{1}{2} Q^{-\frac{v_i+1}{2}+\varepsilon_{2,i}}$, $\varepsilon_{2,i} > 0$ such that $\Pi \subset \bigcup\limits_k \Pi_k$ and $\Pi_k \cap \Pi \neq \emptyset$. Thus, the number K of rectangles Π_k can be estimated as follows

$$K \leq 4 \max\left(\lambda_1(I_1)\left(\lambda_1(J_{1,k})\right)^{-1}, 1\right) \max\left(\lambda_1(I_2)\left(\lambda_1(J_{2,k})\right)^{-1}, 1\right)$$
$$= \begin{cases} 2^4 Q^{\frac{n+1}{2}-\varepsilon_{2,1}-\varepsilon_{2,2}} \lambda_2(\Pi), & s_i < \frac{v_i+1}{2}, \\ 2^4 Q^{\frac{v_1+1}{2}-\varepsilon_{2,1}} \lambda_1(I_1), & s_1 < \frac{v_1+1}{2}, s_2 \geq \frac{v_2+1}{2}, \\ 2^4 Q^{\frac{v_2+1}{2}-\varepsilon_{2,2}} \lambda_1(I_2), & s_1 \geq \frac{v_1+1}{2}, s_2 < \frac{v_2+1}{2}. \end{cases} \tag{3.2.35}$$

We will say that a polynomial P belongs to Π_k if there exists a point $\mathbf{x} \in \Pi_k$ such that the inequalities (3.2.33) hold for polynomial P.

Let us prove that there is no rectangle Π_k containing two or more irreducible polynomials $P \in \mathcal{P}_n(Q)$. Assume the converse: let $P_1, P_2 \in \Pi_k$ be irreducible polynomials and let the inequalities (3.2.33) hold for polynomial P_j at a point $\mathbf{x}_j \in \Pi_k$. Thus, for $Q > Q_0$ and for every point $\mathbf{x} \in \Pi_k$ we have

$$|x_i - \alpha_{j,i}| \leq |x_i - x_{j,i}| + |x_{j,i} - \alpha_{j,i}| \leq Q^{-\frac{v_i+1}{2}+\varepsilon_{2,i}}, \tag{3.2.36}$$

where $x_{j,i} \in S(\alpha_{j,i})$.

Let us estimate the values $|P_j(x_i)|$ for $\mathbf{x} \in \Pi_k$. Consider the Taylor expansion of the polynomial P_j in the interval $J_{i,k}$

$$P_j(x_i) = P_j'(\alpha_{j,i})(x_i - \alpha_{j,i}) + \ldots + \tfrac{1}{n!} P_j^{(n)}(\alpha_{j,i})(x_i - \alpha_{j,i})^n.$$

From the estimates (3.2.33) and (3.2.36) we obtain

$$\left|P_j'(\alpha_{j,i})(x_i - \alpha_{j,i})\right| \ll Q^{-v_i+\frac{v_i}{2(n-1)}+\varepsilon_{2,i}},$$

$$\left|\tfrac{1}{k!} P_j^{(k)}(\alpha_{j,i})(x_i - \alpha_{j,i})^k\right| \ll Q^{1-\frac{k}{2}-\frac{kv_i}{2}+k\varepsilon_{2,i}} \ll Q^{-v_i+\frac{v_i}{2(n-1)}+\varepsilon_{2,i}}$$

for $\varepsilon_{2,i} < \frac{v_i}{2(n-1)^2}$ and $Q > Q_0$. Then any $\varepsilon_3 > 0$ and for $Q > Q_0$ we can write the following estimate

$$|P_j(x_i)| \ll Q^{-v_i+\frac{v_i}{2(n-1)}+\varepsilon_{2,i}} < Q^{-v_i+\frac{v_i}{2(n-1)}+\varepsilon_{2,i}+\varepsilon_3}. \tag{3.2.37}$$

Applying Lemma A.1.16 with $\eta_i = \frac{v_i+1}{2} - \varepsilon_{2,i}$ and $\tau_i = v_i - \frac{v_i}{2(n-1)} - \varepsilon_{2,i} - \varepsilon_3$ we have

$$\tau_1 + \tau_2 + 2 = (n-1) - \tfrac{1}{2} - \varepsilon_{2,1} - \varepsilon_{2,2} + 2 - 2\varepsilon_3 = n + \tfrac{1}{2} - \varepsilon_{2,1} - \varepsilon_{2,2} - 2\varepsilon_3,$$

$$2(\tau_i + 1 - \eta_i) = 2\left(v_i - \tfrac{v_i}{2(n-1)} - \varepsilon_{2,i} - \varepsilon_3 + 1 - \tfrac{v_i+1}{2} + \varepsilon_{2,i}\right) = v_i + 1 - \tfrac{v_i}{n-1} - 2\varepsilon_3.$$

Substituting these expressions into (A.1.4) we get

$$M_{\boldsymbol{\tau},\boldsymbol{\eta}} = 2n + \tfrac{1}{2} - \varepsilon_{2,1} - \varepsilon_{2,2} - 6\varepsilon_3 \geq 2n + \tfrac{1}{8}$$

for $\varepsilon_{2,i} = \frac{v_i}{4(n-1)^2}$ and $\varepsilon_3 = \frac{1}{48}$. This contradicts to Lemma A.1.16 with $\delta = \frac{1}{8}$.

Hence, every rectangle Π_k contains at most one polynomial $P \in \mathcal{P}_n(Q)$ and we have

$$\lambda_2\left(L_{2,2}\right) \leq \sum_{\Pi_k} \lambda_2\left(\sigma_P(\boldsymbol{\alpha})\right).$$

Together with the estimates (3.2.34) and (3.2.35) this leads to

$$\lambda_2\left(L_{2,2}\right) \ll Q^{-\varepsilon_{2,1}-\varepsilon_{2,2}} \lambda_2\left(\Pi\right) < \tfrac{\kappa}{36}\, \lambda_2\left(\Pi\right)$$

for $Q > Q_0$ and $s_i < \frac{v_i+1}{2}$, $i = 1, 2$. If $s_i \geq \frac{v_i+1}{2}$, then for $Q > Q_0$ we obtain

$$\lambda_2\left(L_{2,2}\right) \leq \sum_{P \in \mathcal{P}_n(Q)} \lambda_2\left(\sigma_P(\boldsymbol{\alpha})\right) \ll Q^{-\varepsilon_{2,i}}\, \lambda_1\left(I_1\right)\, \lambda_1\left(I_2\right) < \tfrac{\kappa}{36}\, \lambda_2\left(\Pi\right).$$

3.2.2.4 The case of a small derivative

Let us discuss a situation where $|P'(x_i)| \leq 2c_7\, Q^{\frac{1}{2}-\frac{v_i}{2}}$. In this case, we show that $|P'(\alpha_i)| \leq 3c_7\, Q^{\frac{1}{2}-\frac{v_i}{2}}$, where $x_i \in S(\alpha_i)$.

Indeed, let $|P'(\alpha_i)| > 3c_7\, Q^{\frac{1}{2}-\frac{v_i}{2}}$ and consider a Taylor expansions

$$P'(x_i) = P'(\alpha_i) + P''(\alpha_i)(x_i - \alpha_i) + \ldots + \tfrac{1}{(n-1)!} P^{(n)}(\alpha_i)(x_i - \alpha_i)^{n-1}.$$

Using our assumption and repeating the steps from the beginning of the proof of Lemma 3.2.6 we obtain

$$\left| P''(\alpha_i)(x_i - \alpha_i) + \ldots + \tfrac{1}{(n-1)!} P^{(n)}(\alpha_i)(x_i - \alpha_i)^{n-1} \right| \leq c_7\, Q^{\frac{1}{2}-\frac{v_i}{2}}.$$

This gives us the following contradiction

$$|P'(\alpha_i)| \leq 3c_7\, Q^{\frac{1}{2}-\frac{v_i}{2}}.$$

Now denote by $L_{1,1}$ the set of points $\mathbf{x} \in \Pi$ such that there exists a polynomial $P \in \mathcal{P}_n(Q)$ satisfying

$$\begin{cases} |P(x_i)| < h_n\, Q^{-v_i}, \\ |P'(\alpha_i)| < 3c_7\, Q^{\frac{1}{2}-\frac{v_i}{2}}, \quad i = 1, 2. \end{cases} \tag{3.2.38}$$

We will classify polynomials $P \in \mathcal{P}_n(Q)$ satisfying (3.2.38) according to the distribution of their roots and the size of the leading coefficient. This type of classification was introduced by Sprindžuk [62].

In the rest of the proof we will assume that the roots of the polynomial P are sorted by distance from $\alpha_i = \alpha_{i,1}$

$$|\alpha_{i,1} - \alpha_{i,2}| \leq |\alpha_{i,1} - \alpha_{i,3}| \leq \ldots \leq |\alpha_{i,1} - \alpha_{i,n}|.$$

Let $\varepsilon_4 > 0$ be a sufficiently small constant. For every polynomial $P \in \mathcal{P}_n(Q)$ of degree $3 \le m \le n$ we define the numbers $\omega_{1,j}$ and $\omega_{2,j}$, $2 \le j \le m$ as solutions of the equations

$$|\alpha_{1,1} - \alpha_{1,j}| = Q^{-\omega_{1,j}}, \quad |\alpha_{2,1} - \alpha_{2,j}| = Q^{-\omega_{2,j}}.$$

Let us also define the vectors $\mathbf{k}_i = (k_{i,2}, \dots, k_{i,m}) \in \mathbb{Z}^{m-1}$ as follows

$$(k_{i,j} - 1)\,\varepsilon_4 \le \omega_{i,j} < k_{i,j}\,\varepsilon_4, \quad i = 1, 2, 2 \le j \le m.$$

It is clear, that $k_{i,2} \ge \ldots \ge k_{i,m}$.

Thus, we have $m(m-1)$ pairs of vectors $\mathbf{k}_1, \mathbf{k}_2$ that correspond to a polynomial $P \in \mathcal{P}_n(Q)$ of degree m depending on the choice of roots $\alpha_{1,1}$ and $\alpha_{2,1}$. Let us define subclass of polynomials $\mathcal{P}_m(Q, \mathbf{k}_1, \mathbf{k}_2, u) \subset \mathcal{P}_n(Q)$ as follows. A polynomial P of degree m with leading coefficient a_m belongs to a subclass $\mathcal{P}_m(Q, \mathbf{k}_1, \mathbf{k}_2, u)$, if:

1. the vectors $(\mathbf{k}_1, \mathbf{k}_2)$ correspond to the roots (α_1, α_2) of polynomial P;
2. $Q^u \le |a_m| < Q^{u+\varepsilon_4}$, where $u \in \varepsilon_4\,\mathbb{Z}$.

Let us estimate the number of different subclasses $\mathcal{P}_m(Q, \mathbf{k}_1, \mathbf{k}_2, u)$. First of all, since $1 \le |a_m| \le Q$ we have

$$0 \le u \le 1 - \varepsilon_4.$$

Then from [18, 28] and the natural bound for the roots of polynomial $P \in \mathcal{P}_n(Q)$ we have

$$Q \gg |\alpha_{j_1} - \alpha_{j_2}| \gg H(P)^{-m+1} \gg Q^{-m+1},$$

which leads to the estimate

$$-\frac{1}{\varepsilon_4} + 1 \le k_{i,j} \le \frac{m-1}{\varepsilon_4}.$$

Thus, an integer vector $\mathbf{k}_i$ can take at most $\left(\frac{m}{\varepsilon_4} + 1\right)^{m-1}$ values and the number of subclasses $\mathcal{P}_m(Q, \mathbf{k}_1, \mathbf{k}_2, u)$ can be estimated as follows

$$\#\{m, \mathbf{k}_1, \mathbf{k}_2, u\} \le c_{13}^2(\varepsilon_4^{-1} + 1), \tag{3.2.39}$$

where $c_{13} = \sum\limits_{i=2}^{n} \left(\frac{i}{\varepsilon_4} + 1\right)^{i-1}$. Define the values $p_{i,j}$

$$\begin{cases} p_{i,j} = (k_{i,j+1} + \ldots + k_{i,m})\,\varepsilon_4, & 1 \le j \le m-1, \\ p_{i,j} = 0, \quad j = m. \end{cases} \tag{3.2.40}$$

Using this notation we derive the following estimates for a polynomial $P \in \mathcal{P}_m(Q, \mathbf{k}_1, \mathbf{k}_2, u)$

$$\begin{gathered} Q^{u-p_{i,1}} \le |P'(\alpha_i)| = |a_m| \prod_{k=2}^{m} |\alpha_{i,1} - \alpha_{i,k}| \le Q^{u-p_{i,1}+(m+1)\varepsilon_4}, \\ |P^{(j)}(\alpha_i)| \ll |a_m| \prod_{k=j+1}^{m} |\alpha_{i,1} - \alpha_{i,k}| \ll Q^{u-p_{i,j}+(m+1)\varepsilon_4}, \quad j \ge 2. \end{gathered} \tag{3.2.41}$$

Since we concern only with polynomials satisfying the system (3.2.38), we assume that for at least one value of u the following inequalities hold

$$Q^{u-p_{i,1}} \le |P'(\alpha_i)| \le 3c_7\, Q^{\frac{1}{2}-\frac{v_i}{2}}, \quad i=1,2.$$

This condition implies

$$p_{1,1} > u + \frac{v_1-1}{2}, \qquad p_{2,1} > u + \frac{v_2-1}{2}. \tag{3.2.42}$$

Now let us obtain an estimate for the measure of the set $L_{1,1}$. From Lemma A.1.14 we have

$$L_{1,1} \subset \bigcup_{m,\mathbf{k}_1,\mathbf{k}_2,u} \bigcup_{P\in\mathcal{P}_m(Q,\mathbf{k}_1,\mathbf{k}_2,u)} \bigcup_{\boldsymbol{\alpha}\in\mathcal{A}^2(P)} \sigma_P(\boldsymbol{\alpha}),$$

where

$$\sigma_P(\boldsymbol{\alpha}) := \left\{ \mathbf{x}\in\Pi : \quad |x_i-\alpha_i| \le \min_{1\le j\le m} \left(2^{m-j}\, \frac{h_n\, Q^{-v_i}}{|P'(\alpha_{i,1})|} \prod_{k=2}^{j} |\alpha_{i,1}-\alpha_{i,k}| \right)^{1/j} \right\}.$$

This, together with notation (3.2.40) and the estimates (3.2.41), yields

$$\sigma_P(\boldsymbol{\alpha}) \subset \left\{ \mathbf{x}\in\Pi : |x_i-\alpha_i| \le \tfrac{1}{2} \min_{1\le j\le m} \left((2^m h_n)^{1/j}\, Q^{\frac{-u-v_i+p_{i,j}}{j}} \right) \right\} \tag{3.2.43}$$

for $P\in\mathcal{P}_m(Q,\mathbf{k}_1,\mathbf{k}_2,u)$.

The numbers $j=m_1$ and $j=m_2$ in the formula above provide the best estimates for the roots α_1 and α_2 respectively if for all $1\le k\le m$ the following holds

$$(2^m h_n)^{1/m_i}\, Q^{\frac{-u-v_i+p_{i,m_i}}{m_i}} \le (2^m h_n)^{1/k}\, Q^{\frac{-u-v_i+p_{i,k}}{k}}, \quad i=1,2. \tag{3.2.44}$$

Hence, assuming (3.2.44), we have

$$\sigma_P(\boldsymbol{\alpha}) \subset \left\{ \mathbf{x}\in\Pi : \quad |x_i-\alpha_i| \le \tfrac{1}{2}\, (2^m h_n)^{1/m_i}\, Q^{\frac{-u-v_i+p_{i,m_i}}{m_i}} \right\}. \tag{3.2.45}$$

Let us cover the rectangle Π by a system of disjoint rectangles $\Pi_{m_1,m_2} = J_{m_1}\times J_{m_2}$, where $\lambda_1(J_{m_i}) = \frac{1}{2}\, Q^{-\frac{u+v_i-p_{i,m_i}}{m_i}+\varepsilon_5}$, $\varepsilon_5>0$. The number K of rectangles Π_{m_1,m_2} can be estimated as follows:

$$K \le 2^4\, Q^{\frac{u+v_1-p_{1,m_1}}{m_1}+\frac{u+v_2-p_{2,m_2}}{m_2}-2\varepsilon_5}\, \lambda_2(\Pi). \tag{3.2.46}$$

Let us show that there is no rectangle Π_{m_1,m_2} containing two or more irreducible polynomials. Assume there are two irreducible polynomials P_1,P_2 such that the inequalities (3.2.38) hold for polynomial P_j at points $\mathbf{x}_j\in\Pi_{m_1,m_2}$. Then for all points $\mathbf{x}\in\Pi_{m_1,m_2}$ and for $Q>Q_0$, we obtain

$$|x_i-\alpha_{j,i}| \le |x_i-x_{j,i}| + |x_{j,i}-\alpha_{j,i}| < Q^{-\frac{u+v_i-p_{i,m_i}}{m_i}+\varepsilon_5}, \tag{3.2.47}$$

where $x_{j,i} \in S(\alpha_{j,i})$.

Let us estimate $|P_j(x_i)|$, where $\mathbf{x} \in \Pi_{m_1,m_2}$. Considering a Taylor expansions of the polynomial P_j in the interval J_{m_i} and using estimates (3.2.41), (3.2.44), and (3.2.47) we have

$$\left|\tfrac{1}{k!}\, P_j^{(k)}(\alpha_{j,i})(x_i - \alpha_{j,i})^k\right| \ll Q^{-v_i+(m+1)\varepsilon_4+k\varepsilon_5},$$

and, hence,

$$|P_j(x_i)| \ll Q^{-v_i+(m+1)\varepsilon_4+m\varepsilon_5} < Q^{-v_i+(m+1)(\varepsilon_4+\varepsilon_5)}. \tag{3.2.48}$$

Applying Lemma A.1.16 with $\eta_i = \frac{u+v_i-p_{i,m_i}}{m_i} - \varepsilon_5$ and $\tau_i = v_i - (m+1)(\varepsilon_4+\varepsilon_5)$, and taking $\varepsilon_4 = \frac{1}{12(m+1)}$ and $\varepsilon_5 = \frac{1}{4(3m+1)}$, we obtain

$$\tau_1 + \tau_2 + 2 = n + 1 - \tfrac{1}{6} - 2(m+1)\varepsilon_5,$$

$$2(\tau_i + 1 - \eta_i) = 2v_i + 2 - 2\,\tfrac{u+v_i-p_{i,m_i}}{m_i} - \tfrac{1}{6} - 2m\varepsilon_5.$$

Let us estimate the expression $2(\tau_i + 1 - \eta_i)$ using the inequalities (3.2.42)

$$2(\tau_i+1-\eta_i) \geq \begin{cases} v_i + 2 - u + \frac{2p_{i,m_i}}{m} - \frac{1}{6} - 2m\varepsilon_5, & m_i \geq 2, \\ v_i + 1 - \frac{1}{6} - 2m\varepsilon_5, & m_i = 1, \end{cases} \quad \geq v_i + 1 - \tfrac{1}{6} - 2m\varepsilon_5.$$

Substituting this expressions into (A.1.4) leads to contradiction in Lemma A.1.16 with $\delta = \frac{1}{2}$.

This means that there exists at most one irreducible polynomial $P \in \mathcal{P}_m(Q, \mathbf{k}_1, \mathbf{k}_2, u)$ belonging to the rectangle Π_{m_1,m_2} and, thus,

$$\lambda_2\left(L_{1,1}\right) \leq \sum_{m,\mathbf{k}_1,\mathbf{k}_2,u} \sum_{P\in\mathcal{P}_m(Q,\mathbf{k}_1,\mathbf{k}_2,u)} \lambda_2\left(\sigma_P(\boldsymbol{\alpha})\right) \leq \sum_{m,\mathbf{k}_1,\mathbf{k}_2,u} \sum_{\Pi_{m_1,m_2}} \lambda_2\left(\sigma_P(\boldsymbol{\alpha})\right).$$

Then by estimates (3.2.39), (3.2.45) and (3.2.46) for $Q > Q_0$ we get

$$\lambda_2\left(L_{1,1}\right) \ll Q^{-2\varepsilon_5}\, \lambda_2\left(\Pi\right) < \tfrac{\kappa}{36}\, \lambda_2\left(\Pi\right).$$

3.2.2.5 Mixed cases

The case of sub-intervals $\bar{T}_{1,2}$, $\bar{T}_{2,3}$ ($\bar{T}_{1,3}$, $\bar{T}_{2,2}$)

Consider the system of inequalities

$$\begin{cases} |P(x_i)| < h_n\, Q^{-v_i}, \\ c_7\, Q^{\frac{1}{2}-\frac{v_1}{2}} \leq |P'(\alpha_1)| < 2Q^{\frac{1}{2}-\frac{v_1}{2}+\frac{v_1}{2(n-1)}}, \\ \frac{1}{2} Q^{\frac{1}{2}-\frac{v_2}{2}+\frac{v_2}{2(n-1)}} \leq |P'(\alpha_2)| < 2n\omega_n(3/2\, d_2)\, Q, \quad i = 1, 2. \end{cases} \tag{3.2.49}$$

Denote by $L_{2,3}$ the set of points $\mathbf{x} \in \Pi$ such that the inequalities (3.2.49) hold for some polynomial $P \in \mathcal{P}_n(Q)$.

As in the case of small derivatives, we classify polynomials $P \in \mathcal{P}_n(Q)$ according to the distribution of their roots and the size of their leading coefficients. Let us define subclasses $\mathcal{P}_m(Q, \mathbf{k}_2, u) \subset \mathcal{P}_n(Q)$ as follows. A polynomial P of degree m with leading coefficient a_m belongs to a subclass $\mathcal{P}_m(Q, \mathbf{k}_2, u)$ if:

1. the vector $\mathbf{k}_2$ correspond to the root α_2 of polynomial P;
2. $Q^u \le |a_m| < Q^{u+\varepsilon_4}$, where $u \in \varepsilon_4 \mathbb{Z}$.

Then

$$\#\{m, \mathbf{k}_2, u\} \le c_{13}(\varepsilon_4^{-1} + 1). \tag{3.2.50}$$

Let us fix some m, $\mathbf{k}_2$ and u and denote by $L_m(Q, \mathbf{k}_2, u)$ the set of points $\mathbf{x} \in \Pi$ such that there exists a polynomial $P \in \mathcal{P}_m(Q, \mathbf{k}_2, u)$ satisfying (3.2.49). Then

$$L_{2,3} \subset \bigcup_{m, \mathbf{k}_2, u} L_m(Q, \mathbf{k}_2, u).$$

Define the value $l := v_2 - p_{2,1} + u - k_{2,2}\varepsilon_4$ and let $[l]$ be the integer part and $\{l\}$ be the fractional part of l. Moreover, define the value $\theta := 1 - \{l\} > 0$. Let $L_m^g(Q, \mathbf{k}_2, u)$, $1 \le g \le 2\theta^{-1} + 1$ be the set of points $\mathbf{x} \in \Pi$ such that there exists a polynomial $P \in \mathcal{P}_m(Q, \mathbf{k}_2, u)$ satisfying the system (3.2.49) under condition

$$c_7\, Q^{\frac{1}{2} - \frac{v_1}{2} + \frac{v_1\theta(g-1)}{4(n-1)}} \le |P'(\alpha_1)| < c_7\, Q^{\frac{1}{2} - \frac{v_1}{2} + \frac{v_1 g\theta}{4(n-1)}}.$$

It is clear now that $L_m(Q, \mathbf{k}_2, u) \subset \bigcup_g L_m^g(Q, \mathbf{k}_2, u)$ and, hence,

$$L_{2,3} \subset \bigcup_{m, \mathbf{k}_2, u} \bigcup_g L_m^g(Q, \mathbf{k}_2, u). \tag{3.2.51}$$

By Lemma A.1.14 we obtain

$$L_m^g(Q, \mathbf{k}_2, u) \subset \bigcup_{P \in \mathcal{P}_m(Q, \mathbf{k}_2, u)} \bigcup_{\boldsymbol{\alpha} \in \mathcal{A}^2(P)} \sigma_P(\boldsymbol{\alpha}),$$

where

$$\sigma_P(\boldsymbol{\alpha}) := \left\{ \mathbf{x} \in \Pi : \begin{array}{l} |x_1 - \alpha_1| \le 2^{m-1} h_n\, c_7^{-1}\, Q^{-\frac{v_1}{2} - \frac{1}{2} - \frac{v_1\theta(g-1)}{4(n-1)}}, \\ |x_2 - \alpha_2| \le 2^{m-1} h_n\, Q^{-v_2 + p_{2,1} - u} \end{array} \right\}. \tag{3.2.52}$$

Let us cover the rectangle Π by a system of disjoint rectangles $\Pi_k = J_{1,k} \times J_{2,k}$, where $\lambda_1(J_{1,k}) = \frac{1}{2}\, Q^{-\frac{v_1}{2} - \frac{1}{2} - \frac{v_1\theta(g-1)}{4(n-1)} + \varepsilon_6}$ and $\lambda_1(J_{2,k}) = \frac{1}{2}\, Q^{-k_{2,2}\varepsilon_4 - \{l\}}$. The number K of rectangles $\Pi_k \in \Pi$ can be estimated as

$$K \le 2^4\, Q^{\frac{v_1}{2} + \frac{1}{2} + \frac{v_1\theta(g-1)}{4(n-1)} + k_{2,2}\varepsilon_4 - \varepsilon_6 + \{l\}}\, \lambda_2(\Pi). \tag{3.2.53}$$

Assume that every rectangle Π_k contains at most $2^m Q^{[l]+\frac{\varepsilon_6}{2}}$ polynomials $P_j \in \mathcal{P}_m^g(Q, \mathbf{k}_2, u)$. Then by inequalities (3.2.52) and (3.2.53) we get

$$\begin{aligned}\lambda_2\left(L_m(Q,\mathbf{k}_2,u)\right) &\le \sum_g \lambda_2\left(L_m^g(Q,\mathbf{k}_2,u)\right) \le \sum_g \sum_{\Pi_k} \lambda_2\left(\sigma_P(\boldsymbol{\alpha})\right)\\ &\le 2^{3m+4} h_n^2 c_7^{-1}\left(2\theta^{-1}+1\right) Q^{-v_2+p_{2,1}-u+k_{2,2}\varepsilon_4-\frac{\varepsilon_6}{2}+[l]+\{l\}}\,\lambda_2\left(\Pi\right)\\ &\le Q^{-\frac{\varepsilon_6}{4}}\,\lambda_2\left(\Pi\right),\end{aligned}$$

and, hence, by (3.2.50) and (3.2.51) for $Q > Q_0$ we conclude

$$\lambda_2\left(L_{2,3}\right) \le c_{13}(\varepsilon_4^{-1}+1)\,Q^{-\frac{\varepsilon_6}{4}}\,\lambda_2\left(\Pi\right) \le \tfrac{\kappa}{36}\,\lambda_2\left(\Pi\right). \tag{3.2.54}$$

Now we will show that it is the only possible case and rectangle Π_k can not contain more than $2^m Q^{[l]+\frac{\varepsilon_6}{2}}$ polynomials $P_j \in \mathcal{P}_m^g(Q, \mathbf{k}_2, u)$.

Assume that there exists a rectangle Π_k containing more than $2^m Q^{[l]+\frac{\varepsilon_6}{2}}$ polynomials $P_j \in \mathcal{P}_m^g(Q, \mathbf{k}_2, u)$ and the inequalities (3.2.49) hold for polynomial P_j at point $\mathbf{x}_j \in \Pi_k$. Then for all points $\mathbf{x} \in \Pi_k$ and $Q > Q_0$ we obtain

$$\begin{aligned}|x_2-\alpha_{j,2}| \le |x_2-x_{j,2}| + |x_{j,2}-\alpha_{j,2}| &< Q^{-k_{2,2}\varepsilon_4-\{l\}} + 2^{m-1}h_n\,Q^{-v_2+p_{2,1}-u}\\ &\le Q^{-k_{2,2}\varepsilon_4-\{l\}} + 2^{m-1}h_n\,Q^{-k_{2,2}\varepsilon_4-l} \ll Q^{-k_{2,2}\varepsilon_4-\{l\}},\end{aligned} \tag{3.2.55}$$

where $x_{j,2} \in S(\alpha_{j,2})$.

From the Taylor expansions of polynomials P_j in the interval $J_{2,k}$, the estimates (3.2.41) and (3.2.55) it follows that

$$\begin{aligned}\left|\tfrac{1}{k!}\,P_j^{(k)}(\alpha_{j,2})(x_2-\alpha_{j,2})^k\right| &\ll Q^{u-p_{2,k}+(m+1)\varepsilon_4-k\,k_{2,2}\varepsilon_4-k\{l\}}\\ &< Q^{u-p_{2,1}-k_{2,2}\varepsilon_4-\{l\}+(m+1)\varepsilon_4},\end{aligned}$$

which for $Q > Q_0$ allows us to write

$$|P_j(x_2)| < \tfrac{1}{2}\,Q^{u-p_{2,1}-k_{2,2}\varepsilon_4-\{l\}+(m+2)\varepsilon_4}. \tag{3.2.56}$$

Similarly, repeating the calculations by analogy with Section 3.2.2.3 (see inequality (3.2.37)) for $\varepsilon_6 < \frac{v_1}{(n-1)^2}$, we have

$$|P_j(x_1)| < \tfrac{1}{2}\,Q^{-v_1+\frac{v_1\theta}{4(n-1)}+2\varepsilon_6}. \tag{3.2.57}$$

By pidgeonhole principle we can find at least $N := \left[Q^{\frac{\varepsilon_6}{2}}\right] + 1$ polynomials from $\mathcal{P}_m^g(Q, \mathbf{k}_2, u)$ belonging to Π_k such that their coefficients $a_m, \ldots, a_{m+1-[l]}$ coincide. Let us call them $P_1, \ldots, P_N$. If $[l] = 0$, then we can simply ignore this step. Consider the polynomials $R_{i,j} = P_i - P_j$, $1 \le i < j \le N$ of degree at most $m - [l]$.

From the inequalities (3.2.56) and (3.2.57), we obtain that at every point of the rectangle Π_k the polynomials $R_{i,j}$ satisfy

$$\begin{cases}|R_{i,j}(x_1)| < Q^{-v_1+\frac{v_1\theta}{4(n-1)}+2\varepsilon_6},\\ |R_{i,j}(x_2)| < Q^{u-p_{2,1}-k_{2,2}\varepsilon_4-\{l\}+(m+2)\varepsilon_4},\end{cases} \tag{3.2.58}$$

Assume that among polynomials $R_{i,j}$ we can find at least two polynomials without common roots. Then we can apply Lemma A.1.16 with $\tau_1 = v_1 - \frac{v_1\theta}{4(n-1)} - 2\varepsilon_6$, $\tau_2 = -u + p_{2,1} + k_{2,2}\varepsilon_4 + \{l\} - (m+2)\varepsilon_4$, $\eta_1 = \frac{v_1}{2} + \frac{1}{2} + \frac{v_1\theta(g-1)}{4(n-1)} - \varepsilon_6$, $\eta_2 = k_{2,2}\varepsilon_4 + \{l\}$, so that we have

$$\begin{aligned}
\tau_1 + 1 &= v_1 + 1 - \tfrac{v_1\theta}{4(n-1)} - 2\varepsilon_6,\\
\tau_2 + 1 &= 1 - u + p_{2,1} + k_{2,2}\varepsilon_4 + \{l\} - (m+2)\varepsilon_4,\\
2(\tau_1 + 1 - \eta_1) &= v_1 + 1 - \tfrac{v_1 g\,\theta}{2(n-1)} - 2\varepsilon_6,\\
2(\tau_2 + 1 - \eta_2) &= 2 - 2u + 2p_{2,1} - 2(m+2)\varepsilon_4.
\end{aligned}$$

Substituting these expressions into (A.1.4) yields

$$M_{\boldsymbol{\tau},\boldsymbol{\eta}} = 2v_1 + 5 - \tfrac{v_1\theta(1+2g)}{4(n-1)} + 3p_{2,1} + k_{2,2}\varepsilon_4 - 3u + \{l\} - 3(m+2)\varepsilon_4 - 4\varepsilon_6$$

Using the equation $v_1 = n - 1 - v_2$ and inequality

$$\tfrac{v_1\theta(1+2g)}{4(n-1)} \le \left(\tfrac{3}{4}\theta + 1\right)\tfrac{v_1}{n-1} \le \tfrac{3}{4}\theta + 1,$$

for $\varepsilon_4 = \frac{\theta}{48(m+2)}$ and $\varepsilon_6 \le \frac{\theta}{64}$ we finally obtain

$$\begin{aligned}
M_{\boldsymbol{\tau},\boldsymbol{\eta}} &\ge 2(n - v_2 + p_{2,1} + k_{2,2}\varepsilon_4 - u + \{l\}) + (p_{2,1} - k_{2,2}\varepsilon_4) + (1-u) + \tfrac{1}{8}\theta\\
&\ge 2(m - [l]) + \tfrac{\theta}{8}.
\end{aligned}$$

This inequality contradict to Lemma A.1.16 for $\delta = \frac{\theta}{8} > 0$.

The case when among polynomials $R_{i,j}$, $1 \le i < j \le N+1$ we can not find two polynomials without common roots is considered in [13].

By analogy we can define and consider the set $L_{3,2}$ for the case of sub-intervals $\bar{T}_{1,3}$, $\bar{T}_{2,2}$ and obtain the estimate $\lambda_2(L_{3,2}) \le \frac{\kappa}{36}\lambda_2(\Pi)$.

The case where one derivative is small and the other derivative lies in the sub-interval $\bar{T}_{2,3}$ or $\bar{T}_{2,2}$

Taking into account the estimate for $|P'(\alpha_1)|$ obtained in Section 3.2.2.4 consider the system of inequalities

$$\begin{cases}
|P(x_i)| < h_n\, Q^{-v_i},\\
|P'(\alpha_1)| < 3c_7\, Q^{\frac{1}{2}-\frac{v_1}{2}},\\
\frac{1}{2}Q^{\frac{1}{2}-\frac{v_2}{2}} \le |P'(\alpha_2)| < 2n\omega_n(3/2\, d_2)\, Q, \quad i = 1,2.
\end{cases} \tag{3.2.59}$$

Denote by $L_{1,2}$ the set of points $\mathbf{x} \in \Pi$ such that there exists a polynomial $P \in \mathcal{P}_n(Q)$ satisfying (3.2.59). Let us again classify polynomials $P \in \mathcal{P}_n(Q)$ according to the distribution of their roots and the size of leading coefficients. We will consider the subclasses of polynomials $\mathcal{P}_m(Q, \mathbf{k}_1, \mathbf{k}_2, u)$ defined above.

By analogy with Section 3.2.2.4 (see inequality (3.2.43)) we conclude

$$L_{1,2} \subset \bigcup_{m,\mathbf{k}_1,\mathbf{k}_2,u} \bigcup_{P\in\mathcal{P}_m(Q,\mathbf{k}_1,\mathbf{k}_2,u)} \bigcup_{\boldsymbol{\alpha}\in\mathcal{A}^2(P)} \sigma_P(\boldsymbol{\alpha}),$$

where for $P \in \mathcal{P}_m(Q,\mathbf{k}_1,\mathbf{k}_2,u)$ we have

$$\sigma_P(\boldsymbol{\alpha}) := \left\{ \mathbf{x}\in\Pi : \begin{array}{l} |x_1-\alpha_1| \le \frac{1}{2}\min\limits_{1\le j\le m}\left((2^m h_n)^{1/j}\, Q^{\frac{-u-v_1+p_{1,j}}{j}}\right), \\ |x_2-\alpha_2| \le 2^{m-1}h_n\, Q^{-u-v_2+p_{2,1}} \end{array} \right\}.$$

If the inequalities (3.2.44) hold for $i=1$, then the estimate numbered as $j=m_1$ is optimal for the root α_1, and we have

$$\sigma_P(\boldsymbol{\alpha}) \subset \left\{ \mathbf{x}\in\Pi : \begin{array}{l} |x_1-\alpha_1| \le \frac{1}{2}\,(2^m h_n)^{1/m_1}\, Q^{\frac{-u-v_1+p_{1,m_1}}{m_1}}, \\ |x_2-\alpha_2| \le 2^{m-1}h_n\, Q^{-u-v_2+p_{2,1}} \end{array} \right\}. \tag{3.2.60}$$

Define the value $l := v_2 - p_{2,1} + u - k_{2,2}\varepsilon_4$ as in the previous case and let us cover the rectangle Π by a system of disjoint rectangles $\Pi_k = J_{1,k}\times J_{2,k}$, where $\lambda_1(J_{1,k}) = \frac{1}{2}\,Q^{-\frac{u+v_1-p_{1,m_1}}{m_1}+\varepsilon_7}$ and $\lambda_1(J_{2,k}) = \frac{1}{2}\,Q^{-k_{2,2}\varepsilon_4-\{l\}}$, and estimate the number K of rectangles $\Pi_k\in\Pi$ as follows

$$K \le 2^4\, Q^{\frac{u+v_1-p_{1,m_1}}{m_1}+k_{2,2}\varepsilon_4+\{l\}-\varepsilon_7}\,\lambda_2(\Pi). \tag{3.2.61}$$

Assume that every rectangle Π_k contains at most $2^m\,Q^{[l]+\frac{\varepsilon_7}{2}}$ polynomials $P\in\mathcal{P}_m(Q,\mathbf{k}_1,\mathbf{k}_2,u)$. Then by inequalities (3.2.59), (3.2.39), and (3.2.61) for $Q>Q_0$ we get

$$\lambda_2(L_{1,2}) \ll Q^{-u-v_2+p_{2,1}+k_{2,2}\varepsilon_4-\frac{\varepsilon_7}{2}+[l]+\{l\}}\,\lambda_2(\Pi) \ll Q^{-\frac{\varepsilon_7}{2}}\,\lambda_2(\Pi) \le \tfrac{\kappa}{18}\,\lambda_2(\Pi).$$

Now assume that there exists a rectangle Π_k containing more than $2^m\,Q^{[l]+\frac{\varepsilon_7}{2}}$ polynomials $P_j\in\mathcal{P}_m(Q,\mathbf{k}_1,\mathbf{k}_2,u)$. Using the calculations described in the previous case (see estimate (3.2.54)) and in Section 3.2.2.4 (see estimate (3.2.48)) for every point $\mathbf{x}\in\Pi_k$ we obtain

$$|P_j(x_1)| < \tfrac{1}{2}\,Q^{-v_1+(m+1)(\varepsilon_4+\varepsilon_7)}, \quad |P_j(x_2)| < \tfrac{1}{2}\,Q^{u-p_{2,1}-k_{2,2}\varepsilon_4-\{l\}+(m+2)\varepsilon_4}. \tag{3.2.62}$$

By pidgeonhole principle we can find at least $N := \left[Q^{\frac{\varepsilon_7}{2}}\right]+1$ polynomials $P_j\in\mathcal{P}_m(Q,\mathbf{k}_1,\mathbf{k}_2,u)$ belonging to Π_k such that their coefficients $a_m,\dots,a_{m+1-[l]}$ coincide. Thus, let us consider the differences $R_{i,j}=P_i-P_j$, $1\le i<j\le N$, which are polynomials of degree at most $m-[l]$.

Using inequalities (3.2.62), we conclude that for every point $\mathbf{x}\in\Pi_k$ the following holds

$$\begin{cases} |R_{i,j}(x_1)| < Q^{-v_1+(m+1)(\varepsilon_4+\varepsilon_7)}, \\ |R_{i,j}(x_2)| < Q^{u-p_{2,1}-k_{2,2}\varepsilon_4-\{l\}+(m+2)\varepsilon_4}, \end{cases}$$

Assume that among polynomials $R_{i,j}$ we can find at least two polynomials without common roots and apply Lemma A.1.16 with $\tau_1 = v_1 - (m+1)(\varepsilon_4+\varepsilon_7)$, $\tau_2 = -u + p_{2,1} + k_{2,2}\,\varepsilon_4 + \{l\} - (m+2)\varepsilon_4$, $\eta_1 = \frac{u+v_1-p_{1,m_1}}{m_1} - \varepsilon_7$, $\eta_2 = k_{2,2}\varepsilon_4 + \{l\}$, so that we have

$$\begin{aligned}\tau_1 + 1 &= v_1 + 1 - (m+1)(\varepsilon_4+\varepsilon_7),\\ \tau_2 + 1 &= 1 - u + p_{2,1} + k_{2,2}\varepsilon_4 + \{l\} - (m+2)\varepsilon_4.\end{aligned}$$

Repeating the arguments from the end of Section 3.2.2.4 we obtain

$$\begin{aligned}2(\tau_1 + 1 - \eta_1) &\geq v_1 + 1 - 2(m+1)\varepsilon_4 - 2m\varepsilon_7,\\ 2(\tau_2 + 1 - \eta_2) &= 2 - 2u + 2p_{2,1} - 2(m+2)\varepsilon_4.\end{aligned}$$

Substituting these expressions into (A.1.4) for $\varepsilon_4 = \frac{1}{48(m+2)}$ and $\varepsilon_7 = \frac{1}{8(3m+1)}$ yields

$$\begin{aligned}M_{\boldsymbol{\tau},\boldsymbol{\eta}} &\geq 2v_1 + 5 + 3p_{2,1} + k_{2,2}\varepsilon_4 - 3u + \{l\} - \tfrac{1}{4}\\ &\geq 2n - 2v_2 + 2p_{2,1} + 2k_{2,2}\varepsilon_4 - 2u + \{l\} + \tfrac{7}{4} \geq 2(m - [l]) - \{l\} + 1 + \tfrac{3}{4}\\ &\geq 2(m - [l]) + \tfrac{3}{4}.\end{aligned}$$

This inequality contradicts to Lemma A.1.16 with $\delta = \frac{3}{4}$.

If among polynomials $R_{i,j}$, $1 \leq i < j \leq N$ we can not find two polynomials without common roots then we use the arguments described in [13].

By analogy we can define and consider the set $L_{2,1}$ for the case when one derivative is small and the other derivative lies in the sub-interval $\bar{T}_{1,3}$ or $\bar{T}_{1,2}$ and obtain the estimate $\lambda_2(L_{2,1}) \leq \frac{\kappa}{18}\,\lambda_2(\Pi)$.

Thus, we have $L_1 \subset \bigcup\limits_{1\leq i,j\leq 2} L_{i,j}$, which leads to the following estimate

$$\lambda_2(L_1) \leq \sum_{1\leq i,j\leq 2} \lambda_2(L_{i,j}) + \lambda_2(L_{3,3}) + \lambda_2(L_{2,3}) + \lambda_2(L_{3,2}) \leq \tfrac{\kappa}{4}\,\lambda_2(\Pi)\,.$$

Similarly, $\lambda_2(L_2) \leq \frac{\kappa}{4}\,\lambda_2(\Pi)$. These estimates conclude the proof of Lemma 3.2.6 in the case of irreducible polynomials.

3.2.2.6 The case of reducible polynomials

In this section we will estimate the measure of the set L_3. Clearly, the results of Lemma A.1.16 can not be applied directly in this case. Let a polynomial P of degree n be a product of several (not necessarily different) irreducible polynomials $P_1, P_2, \ldots, P_m$, $m \geq 2$, where $\deg P_i = n_i$ and $n_1 + \ldots + n_m = n$. Then by Lemma A.1.17 and definition of the height function we have

$$H(P_i) \leq H(P_1)\,H(P_2)\cdot\ldots\cdot H(P_m) \leq c_{14}\,H(P) \leq c_{14}\,Q =: Q_1.$$

Denote by $L_3(k,\varepsilon_8)$ the set of points $\mathbf{x}\in\Pi$ such that there exists a polynomial $R\in\mathcal{P}_k(Q_1)$ satisfying the inequality

$$|R(x_1)R(x_2)|<h_n^2\,Q_1^{-k+\varepsilon_8}. \tag{3.2.63}$$

If a polynomial P satisfies the inequalities (3.2.5) at a point $\mathbf{x}\in\Pi$, we can write

$$|P(x_1)P(x_2)|=|P_1(x_1)P_1(x_2)|\cdot\ldots\cdot|P_s(x_1)P_s(x_2)|\le h_n^2\,Q^{-n+1}. \tag{3.2.64}$$

Since $n=n_1+\ldots+n_m$ and $m\ge 2$, it is easy to see that at least one of the inequalities

$$\begin{aligned}&|P_i(x_1)P_i(x_2)|\le h_n^2\,Q^{-n_i+\varepsilon_8},\quad n_i\ge 2,\\ &|P_i(x_1)P_i(x_2)|\le h_n^2\,Q^{-\varepsilon_8},\quad n_i=1, i=1,\ldots,m,\end{aligned} \tag{3.2.65}$$

hold at the point $\mathbf{x}$ for $1>\varepsilon_8>\frac{1}{2}$. Indeed, without loss of generality assume that $n_1=\ldots=n_{m_1}=1$ and $1<n_{m_1+1}\le\ldots\le n_m$ and assume that the inequalities (3.2.65) do not hold for any $i=1,\ldots,m$ then

$$|P(x_1)P(x_2)|\ge h_n^{2m}\,Q^{-n+m_1+(m-2m_1)\varepsilon_8}\ge h_n^{2m}\,Q^{-n+\frac{m}{2}}\ge h_n^{2m}\,Q^{-n+1},$$

which contradicts to (3.2.64). Hence, $\mathbf{x}\in L_3\,(n_j,\varepsilon_8)$ for $n_j\ge 2$ or $\mathbf{x}\in L_3\,(1,1-\varepsilon_8)$ and we have

$$L_3\subset\left(\bigcup_{k=2}^{n-1}L_3(k,\varepsilon_8)\right)\cup L_3(1,1-\varepsilon_8).$$

Let us estimate the measure of the set $L_3(k,\varepsilon_8)$, $2\le k\le n-1$. Denote by $L_3^1(k,t)$ the set of points $\mathbf{x}\in\Pi$ such that there exists a polynomial $P\in\mathcal{P}_k(Q_1)$ satisfying the inequalities

$$\begin{cases}|P(x_1)|<h_n^2\,Q_1^t,\\ |P(x_2)|<h_n^2\,Q_1^{-k+1-t},\\ \min\limits_i\{|P'(\alpha_i)|\}<\delta_k\,Q_1,\quad x_i\in S(\alpha_i), i=1,2.\end{cases} \tag{3.2.66}$$

Denote by $L_3^2(k,t)$ the set of points $\mathbf{x}\in\Pi$ such that there exists a polynomial $P\in\mathcal{P}_k(Q_1)$ satisfying the inequalities

$$\begin{cases}|P(x_1)|<h_n^2\,Q_1^t,\\ |P(x_2)|<h_n^2\,Q_1^{-k+\frac{1+\varepsilon_8}{2}-t},\\ |P'(\alpha_i)|>\delta_k\,Q_1,\quad x_i\in S(\alpha_i),\quad i=1,2.\end{cases} \tag{3.2.67}$$

By the definition of the set $L_3(k,\varepsilon_8)$ it is easy to see that

$$L_3(k,\varepsilon_8)\subset\left(\bigcup_{i=0}^{N_1}L_3^1(k,1-i(1-\varepsilon_8))\right)\cup\left(\bigcup_{i=0}^{N_2}L_3^2(k,1-i(1-3\varepsilon_8)/2)\right),$$

where $N_1 = \left[\frac{2+k-\varepsilon_8}{1-\varepsilon_8}\right]$ and $N_2 = \left[\frac{4+2k-2\varepsilon_8}{1-3\varepsilon_8}\right]$.

The system (3.2.66) is a system of the form (3.2.5). Furthermore, since the polynomials $P \in \mathcal{P}_k(Q_1)$ are irreducible and $k < n$, we can apply the above arguments for a sufficiently small constant δ_k and $Q_1 > Q_0$ to obtain the following estimate

$$\lambda_2\left(L_3^1(k,t)\right) < \tfrac{\kappa}{2n(N_1+1)}\,\lambda_2\left(\Pi\right). \tag{3.2.68}$$

Now let us estimate the measure of the set $L_3^2(k,t)$. From Lemma A.1.14 we have

$$L_3^2(k,t) \subset \bigcup_{P\in\mathcal{P}_k(Q_1)}\ \bigcup_{\boldsymbol{\alpha}\in\mathcal{A}^2(P)} \sigma_P(\boldsymbol{\alpha},t),$$

where

$$\sigma_P(\boldsymbol{\alpha},t) := \left\{\mathbf{x}\in\Pi:\ \begin{matrix} |x_1-\alpha_1| \le 2^{k-1}h_n^2\,Q_1^t\,|P'(\alpha_1)|^{-1}, \\ |x_2-\alpha_2| \le 2^{k-1}h_n^2\,Q_1^{-k+\frac{1+\varepsilon_8}{2}-t}\,|P'(\alpha_2)|^{-1}. \end{matrix}\right\}$$

Let us estimate the value of the polynomial P at the middle point $\mathbf{d}$ of the rectangle Π. Consider a Taylor expansion

$$P(d_i) = P'(\alpha_i)(d_i-\alpha_i) + \tfrac{1}{2}P''(\alpha_i)(d_i-\alpha_i)^2 + \ldots + \tfrac{1}{k!}\,P^{(k)}(\alpha_i)(d_i-\alpha_i)^k. \tag{3.2.69}$$

If polynomial P satisfy (3.2.67) at point $\mathbf{x}_0 \in \Pi$ then

$$\begin{aligned} &|d_1-\alpha_1| \le \lambda_1\left(I_1\right) + 2^{k-1}h_n^2\delta_k^{-1}\,Q_1^{t-1}, \\ &|d_2-\alpha_2| \le \lambda_1\left(I_2\right) + 2^{k-1}h_n^2\delta_k^{-1}\,Q_1^{-k+\frac{1+\varepsilon_8}{2}-t-1}. \end{aligned} \tag{3.2.70}$$

Without loss of generality, let us assume that $t \ge -k+\frac{1+\varepsilon_8}{2}-t$. Then we can rewrite the estimates (3.2.70) as follows:

$$|d_1-\alpha_1| \le \begin{cases} c_{15}\,\lambda_1\left(I_1\right), & t < 1-s_1, \\ c_{15}\,Q_1^{t-1}, & 1-s_1 \le t \le 1, \end{cases} \qquad |d_2-\alpha_2| \le \lambda_1\left(I_2\right).$$

where $c_{15} = 2^{k-1}h_n^2\delta_k^{-1} + c_{1,1}$. We remind that $\lambda_1\left(I_i\right) = c_{1,i}\,Q^{-s_i}$ and $s_1 \le s_2$.

Using these inequalities and expression (3.2.69) allows us to write

$$|P(d_1)| < \begin{cases} c_{16}\,Q_1\,\lambda_1\left(I_1\right), & t < 1-s_1, \\ c_{16}\,Q_1^t, & 1-s_1 \le t \le 1, \end{cases} \qquad |P(d_2)| < c_{16}\,Q_1\,\lambda_1\left(I_2\right). \tag{3.2.71}$$

Fix a vector $\mathbf{a} = (a_k,\ldots,a_2) \in \mathbb{Z}^{k-1}$ and consider a subclass $\mathcal{P}_k(\mathbf{a})$ of polynomials P which satisfy (3.2.67) and have the same vector of coefficients $\mathbf{a}$, namely $P(t) = a_kt^k+\ldots+a_2t^2+a_1t+a_0$. For $Q_1 > Q_0$, the number of such classes can be estimated as follows

$$\#\left([-Q_1;Q_1]^{k-1}\cap\mathbb{Z}^{k-1}\right) = (2Q_1+1)^{k-1} < 2^k\,Q_1^{k-1}. \tag{3.2.72}$$

Let us estimate the value $\#\mathcal{P}_k(\mathbf{a})$. Choose a polynomial $P_0 \in \mathcal{P}_k(\mathbf{a})$ and consider the difference between the polynomials P_0 and $P_j \in \mathcal{P}_k(\mathbf{a})$ at points d_i. By (3.2.71) we have

$$|(a_{0,1} - a_{j,1})d_1 + (a_{0,0} - a_{j,0})| \le \begin{cases} 2c_{16}\, Q_1 \lambda_1\left(I_1\right), & t < 1 - s_1, \\ 2c_{16}\, Q_1^t, & 1 - s_1 \le t \le 1, \end{cases}$$

$$|(a_{0,1} - a_{j,1})d_2 + (a_{0,0} - a_{j,0})| \le 2c_{16}\, Q_1 \lambda_1\left(I_2\right).$$

This implies that the number of different polynomials $P_j \in \mathcal{P}_k(\mathbf{a})$ does not exceed the number of integer solutions of the system

$$|b_1 d_i + b_0| \le K_i, \quad i = 1, 2,$$

where $K_2 = 2c_{16}\, Q_1 \lambda_1\left(I_2\right)$ and $K_1 = 2c_{16}\, Q_1 \lambda_1\left(I_1\right)$ if $t < 1 - s_1$ and $K_1 = 2c_{16}\, Q_1^t$ if $1 - s_1 \le t \le 1$.

It is easy to see that $K_i \ge 2c_{16}\, Q_1^{1-s_1} > Q_1^{\varepsilon_9}$ for $Q_1 > Q_0$. Thus, by Lemma 3.2.5 we have

$$\#\mathcal{P}_k(\mathbf{a}) \le \begin{cases} 2^7 \varepsilon_1^{-1}\, Q_1^2\, \lambda_2\left(\Pi\right), & t < 1 - s_1, \\ 2^7 \varepsilon_1^{-1}\, Q_1^{t+1}\, \lambda_1\left(I_2\right), & 1 - s_1 \le t \le 1. \end{cases}$$

This estimate and the inequality (3.2.72) mean that the number N of polynomials $P \in \mathcal{P}_k(Q_1)$ satisfying the system (3.2.67) can be estimated as follows

$$N \le \begin{cases} 2^{k+7} \varepsilon_1^{-1}\, Q_1^{k+1}\, \lambda_2\left(\Pi\right), & t < 1 - s_1, \\ 2^{k+7} \varepsilon_1^{-1}\, Q_1^{k+t}\, \lambda_1\left(I_2\right), & 1 - s_1 \le t \le 1. \end{cases} \tag{3.2.73}$$

On the other hand, the measure of the set $\sigma_P(\boldsymbol{\alpha}, t)$ satisfies the inequality

$$\lambda_2\left(\sigma_P(\boldsymbol{\alpha}, t)\right) \le \begin{cases} 2^{2k} h_n^4 \delta_k^{-2}\, Q_1^{-k-2+\frac{1+\varepsilon_8}{2}}, & t < 1 - s_1, \\ 2^{2k} h_n^4 \delta_k^{-2}\, Q_1^{-k-1-t+\frac{1+\varepsilon_8}{2}}\, \lambda_1\left(I_1\right), & 1 - s_1 \le t \le 1. \end{cases} \tag{3.2.74}$$

Then, by estimates (3.2.73) and (3.2.74), for $Q_1 > Q_0$ we get

$$\lambda_2\left(L_3^2(k, t)\right) \le 2^{3k+7} \delta_k^{-2} h_n^4 \varepsilon_1^{-1}\, Q_1^{-\frac{1-\varepsilon_8}{2}}\, \lambda_2\left(\Pi\right) < \tfrac{\kappa}{2n(N_2+1)}\, \lambda_2\left(\Pi\right). \tag{3.2.75}$$

The inequalities (3.2.68) and (3.2.75) lead to the following estimate

$$\lambda_2\left(L_3(k, \varepsilon_8)\right) \le \tfrac{\kappa}{2n}\, \lambda_2\left(\Pi\right).$$

Now let us estimate the measure of the set $L_3(1, 1 - \varepsilon_8)$ for $\varepsilon_8 \ge \max(s_1, s_2, 1/2)$. For every point $\mathbf{x} \in L_3(1, 1 - \varepsilon_8)$ there exists a rational point $\frac{a_0}{a_1}$ such that

$$\left|x_1 - \tfrac{a_0}{a_1}\right| \left|x_2 - \tfrac{a_0}{a_1}\right| < h_n^2\, Q_1^{-\varepsilon_8} |a_1|^{-2}.$$

Since $|x_1 - x_2| > \varepsilon_1$ one of the values $\left|x_i - \frac{a_0}{a_1}\right|$ is bigger than $\frac{\varepsilon_1}{2}$. Thus, we consider the sets

$$\sigma_i\left(a_0/a_1\right) := \left\{\mathbf{x} \in \Pi : \left|x_i - \tfrac{a_0}{a_1}\right| \le 2h_n^2\varepsilon_1^{-1}\, Q_1^{-\varepsilon_8}|a_1|^{-2}\right\}, \quad i = 1, 2. \tag{3.2.76}$$

Simple calculations show that for $c_{1,1}c_{1,2} > 4h_n^2\varepsilon_1^{-1}$ we have

$$\mu_2\sigma_i\left(a_0/a_1\right) \le 4h_n^2\varepsilon_1^{-1}\, Q_1^{-2\varepsilon_8} \le \mu_2\Pi.$$

Let us define the following sets

$$\sigma_i = \bigcup_{1\le a_0,a_1\le Q_1} \sigma_i\left(a_0/a_1\right), \quad i = 1, 2.$$

It is easy to see that $L_3(1, 1-\varepsilon_8) \subset (\sigma_1 \cup \sigma_2)$ and we need to estimate the measure of the sets σ_1 and σ_2.

For a fixed value a_1 let us consider the set $N(a_1) := \{a_0 \in \mathbb{Z} : \sigma_i\left(a_0/a_1\right) \ne \varnothing\}$. The cardinality of this set can be estimated by the following way

$$\#N(a_1) \le \begin{cases} 3\lambda_1\left(I_i\right)|a_1|, & \frac{1}{\lambda_1(I_i)} \le |a_1| \le Q_1, \\ 2, & 1 \le |a_1| < \frac{1}{\lambda_1(I_i)}. \end{cases}$$

These inequalities together with (3.2.76) imply

$$\begin{aligned}
\lambda_2\left(\sigma_i\right) &\le \sum_{1\le|a_1|\le Q_1} N(a_1)\,\lambda_2\left(\sigma_i\left(a_0/a_1\right)\right) \\
&\le 8h_n^2\varepsilon_1^{-1}\, Q_1^{-\varepsilon_8}\,\lambda_1\left(I_i\right) \sum_{1\le|a_1|<\left(\lambda_1(I_i)\right)^{-1}} |a_1|^{-2} \\
&+ 12h_n^2\varepsilon_1^{-1}\, Q_1^{-\varepsilon_8}\,\lambda_2\left(\Pi\right) \sum_{\left(\lambda_1(I_i)\right)^{-1}\le|a_1|\le Q_1} |a_1|^{-1} \\
&\le 2\pi^2 h_n^2\varepsilon_1^{-1}\, Q_1^{-\varepsilon_8}\,\lambda_1\left(I_i\right) + 12h_n^2\varepsilon_1^{-1}\, Q_1^{-\varepsilon_8} \ln Q_1 \lambda_2\left(\Pi\right) \le \tfrac{\kappa}{4n}\,\lambda_2\left(\Pi\right)
\end{aligned}$$

for $Q_1 > Q_0$ and $\varepsilon_8 > \max(s_1, s_2)$. Then,

$$\lambda_2\left(L_3(1, 1-\varepsilon_8)\right) \le \tfrac{\kappa}{2n}\,\lambda_2\left(\Pi\right),$$

and, finally, choosing $\varepsilon_8 > \max(s_1, s_2, 1/2)$, we obtain

$$\lambda_2\left(L_3\right) \le \sum_{k=2}^{n-1} \lambda_2\left(L_3(k, \varepsilon_8)\right) + \lambda_2\left(L_3(1, 1-\varepsilon_8)\right) \le \tfrac{\kappa}{2}\,\lambda_2\left(\Pi\right).$$

This proves Lemma 3.2.6 in case of reducible polynomials.

Combining estimates for the different cases yields the final estimate

$$\lambda_2\left(L\right) \le \lambda_2\left(L_1\right) + \lambda_2\left(L_2\right) + \lambda_2\left(L_3\right) \le \kappa\,\lambda_2\left(\Pi\right).$$

□

Remark 3.2.7. *Note, that in case of reducible polynomials we do not use the inequality* $\min\limits_i \{|P'(x_i)|\} < \delta_n Q$. *It means, that the set* L_3 *is the set of points* $\mathbf{x} \in \Pi$ *such that there exists a reducible polynomial* $P \in \mathcal{P}_n(Q)$ *satisfying the inequalities*

$$|P(x_i)| < h_n Q^{-v_i}, \quad i = 1, 2.$$

3.2.2.7 The final part of the proof

Let us use Lemma 3.2.6 to finish the proof. Consider a set $B_1 := \Pi \setminus L_n(Q, \delta_n, \mathbf{v}, \Pi)$ for $n \geq 2$, $v_1 = v_2 = \frac{n-1}{2}$, $\kappa = \frac{1}{4}$, $Q > Q_0$, $h_n = \sqrt{\frac{3}{2}}(|d_1| + |d_2|)^{1/2} \max(1, 3|d_1|, 3|d_2|)^{n^2/2}$ and a sufficiently small constant δ_n. From Lemma 3.2.6 it follows that

$$\lambda_2(B_1) \geq \tfrac{3}{4} \lambda_2(\Pi). \tag{3.2.77}$$

Let us prove that for every point $\mathbf{x} \in \Pi$ there exists a polynomial $P \in \mathcal{P}_n(Q)$ satisfying

$$|P(x_i)| \leq h_n Q^{-\frac{n-1}{2}}, \quad i = 1, 2.$$

By Minkowski's linear forms theorem (Lemma A.2.3) for every point $\mathbf{x} \in \Pi$ there exists a non-zero polynomial $P(t) = a_n t^n + \ldots + a_1 t + a_0 \in \mathbb{Z}[t]$ satisfying

$$|P(x_i)| \leq h_n Q^{-\frac{n-1}{2}}, \quad |a_j| \leq \max(1, 3|d_1|, 3|d_2|)^{-n-1} Q \quad (i = 1, 2, \quad 2 \leq j \leq n).$$

One can easily verify that $|a_1| < Q$ and $|a_0| < Q$, hence $P \in \mathcal{P}_n(Q)$.

Then, by Remark 3.2.7 we conclude that for every point $\mathbf{x}_1 \in B_1$ there exists an irreducible polynomial $P_1 \in \mathcal{P}_n(Q)$ satisfying

$$\begin{cases} |P_1(x_{1,i})| < h_n Q^{-\frac{n-1}{2}}, \\ |P_1'(x_{1,i})| > \delta_n Q, \quad i = 1, 2. \end{cases}$$

Consider the roots α_1, α_2 of the polynomial P_1 such that $x_{1,i} \in S(\alpha_i)$. By Lemma 3.2.4, we have

$$|x_{1,i} - \alpha_i| \leq n h_n \delta_n^{-1} Q^{-\frac{n+1}{2}}, \quad i = 1, 2. \tag{3.2.78}$$

Let us prove that $\alpha_1, \alpha_2 \in \mathbb{R}$. Assume the converse: let $\alpha_i \in \mathbb{C}$, then its complex conjugate $\bar{\alpha}_i$ is also the root of the polynomial P_1, and $x_{1,i} \in S(\bar{\alpha}_i)$. Hence, from the estimates (3.2.78) and Lemma A.1.18 we have

$$|P'(\alpha_i)| \leq |a_n||\bar{\alpha}_i - \alpha_i| \leq c_{17} Q^{-\frac{n-1}{2}}.$$

On the other hand, a Taylor expansion of the polynomial P_1 in the interval $S(\alpha_i)$ implies that

$$|P'(\alpha_i)| \geq \tfrac{1}{2} \delta_n Q.$$

These two inequalities contradict each other.

Let us choose a maximal system of points with algebraic conjugate coordinates $\Gamma = \{\boldsymbol{\gamma}_1, \dots, \boldsymbol{\gamma}_t\}$ satisfying the condition that rectangles

$$\sigma(\boldsymbol{\gamma}_k) = \left\{\mathbf{x} \in \mathbb{R}^2 \colon |x_i - \gamma_{k,i}| < n\delta_n^{-1} Q^{-\frac{n+1}{2}}, i = 1, 2\right\}, \quad 1 \le k \le t,$$

do not intersect. Furthermore, let us introduce expanded rectangles

$$\sigma'(\boldsymbol{\gamma}_k) = \left\{\mathbf{x} \in \mathbb{R}^2 \colon |x_i - \gamma_{k,i}| < 2nh_n\delta_n^{-1} Q^{-\frac{n+1}{2}}, i = 1, 2\right\}, \quad 1 \le k \le t, \quad (3.2.79)$$

and show that

$$B_2 \subset \bigcup_{k=1}^{t} \sigma'(\boldsymbol{\gamma}_k). \quad (3.2.80)$$

To prove this fact, we will show that for any point $\mathbf{x}_1 \in B_1$ there exists a point $\boldsymbol{\gamma}_k \in \Gamma$ such that $\mathbf{x}_1 \in \sigma'(\boldsymbol{\gamma}_k)$. Since $\mathbf{x}_1 \in B_1$, there is a point $\boldsymbol{\alpha}$ satisfying the inequalities (3.2.78). Thus, either $\boldsymbol{\alpha} \in \Gamma$ and $\mathbf{x}_1 \in \sigma'(\boldsymbol{\alpha})$, or there exists a point $\boldsymbol{\gamma}_k \in \Gamma$ satisfying

$$|\alpha_i - \gamma_{k,i}| \le nh_n\delta_n^{-1} Q^{-\frac{n+1}{2}}, \quad i = 1, 2,$$

which implies that $\mathbf{x}_1 \in \sigma'(\boldsymbol{\gamma}_k)$. Hence, from (3.2.77),(3.2.79) and (3.2.80) we have

$$\tfrac{3}{4}\,\lambda_2(\Pi) \le \lambda_2(B_1) \le \sum_{k=1}^{t} \lambda_2(\sigma_1(\boldsymbol{\gamma}_k)) \le t\,2^6 n^2 h_n^2 \delta_n^{-2} Q^{-n-1},$$

which yields the estimate

$$\mathcal{N}_n^2(\mathbb{A}, Q, \Pi) \ge t \ge c_2\, Q^{n+1} \lambda_2(\Pi).$$

3.2.3 Proof of Theorem 3.2.2: Lower Bound

The proof of Theorem 3.2.2 is based on the following lemma.

Lemma 3.2.8. *Given a vector $\mathbf{v} = (v_1, v_2) \in \mathbb{R}_+^2$ with $v_1 + v_2 = n-1$ consider some $\left(\frac{v_1}{n-1}, \frac{v_2}{n-1}\right)$- ordinary square $\overline{\Pi} = I_1 \times I_2$ with middle point $\mathbf{d} = (d_1, d_2)$, $d_1 \ne d_2$ satisfying the conditions:*

- $\lambda_1(I_1) = \lambda_1(I_2) = c_3\, Q^{-s}$, *where* $\frac{1}{2} < s < \frac{3}{4}$;
- $c_3 > c_0(n, \mathbf{d}) > 0$;

and denote by $L := L(Q, \delta_n, \kappa, \mathbf{v}, \overline{\Pi})$ the set of points $\mathbf{x} \in \Pi$ such that there exists a polynomial $P \in \mathcal{P}_n(Q)$ satisfying the inequalities

$$\begin{cases} |P(x_i)| < h_n\, Q^{-v_i}, \\ \min\limits_i \{|P'(x_i)|\} < \delta_n\, Q, \quad i = 1, 2. \end{cases} \quad (3.2.81)$$

Then for any $0 < \kappa < 1$, any $0 < \delta_n \le \delta_0(n, \mathbf{d}, \kappa)$, and any positive $Q > Q_0(n, \mathbf{s}, \mathbf{v}, \mathbf{d}, \kappa)$ we have

$$\lambda_2(L) < \kappa\, \lambda_2\left(\overline{\Pi}\right).$$

Proof. The proof of Lemma 3.2.8 is analogous to the proof of Lemma 3.2.6, except for the base of induction.

3.2.3.1 The base of induction: polynomials of the second degree.

Consider the system (3.2.81) for $n = 2$. Given some $\gamma_{2,1}, \gamma_{2,2} > 0$ under condition $\gamma_{2,1} + \gamma_{2,2} = 1$ and an $(\gamma_{2,1}, \gamma_{2,2})$- ordinary square $\overline{\Pi} = I_1 \times I_2$ under conditions of Lemma 3.2.8 denote by $L' := L_2(Q, \delta_2, \kappa, \boldsymbol{\gamma}_2, \overline{\Pi})$ the set of points $\mathbf{x} \in \overline{\Pi}$ such that there exists a polynomial $P \in \mathcal{P}_2(Q)$ satisfying inequalities

$$\begin{cases} |P(x_i)| < h_2\, Q^{-\gamma_{2,i}}, \\ \min\limits_i \{|P'(x_i)|\} < \delta_2\, Q, \quad i = 1, 2, \\ |b_2| > Q^{s-\frac{1}{2}}. \end{cases} \tag{3.2.82}$$

We will show that for any $\delta_2 < \delta_0(\mathbf{d}, \mathbf{s}, \kappa)$ and any $Q > Q_0(\mathbf{s}, \kappa, \boldsymbol{\gamma}_2, \mathbf{d})$ we have

$$\lambda_2\left(L'\right) < \kappa\, \lambda_2\left(\overline{\Pi}\right).$$

Consider a polynomial $P(t) = b_2t^2 + b_1t + b_0 \in \mathcal{P}_2(Q)$. Applying the same argument as we used in Subsection 3.2.2.1, we obtain upper and lower bounds for the absolute value of the derivative P' at roots α_1, α_2 and at points x_1, x_2, where $x_i \in S(\alpha_i)$

$$|P'(\alpha_i)| > \tfrac{3}{4}\,\varepsilon\,|b_2|, \quad |P'(x_i)| \le \left(|d_1| + |d_2| + 1 + \tfrac{\varepsilon}{4}\right)|b_2|. \tag{3.2.83}$$

These estimates lead to the following inequality

$$|b_2| < 4\delta_2\varepsilon^{-1}\, Q.$$

From Lemma A.1.14 and the estimates (3.2.82), (3.2.83) it follows that L' is a subset of a union $\bigcup\limits_{P \in \mathcal{P}_2(Q)} \sigma_P$, where

$$\sigma_P := \left\{\mathbf{x} \in \overline{\Pi} : \quad |x_i - \alpha_i| < 2h_2\varepsilon^{-1}\, Q^{-\gamma_{2,i}}|b_2|^{-1}, i = 1, 2\right\}. \tag{3.2.84}$$

Since the square $\overline{\Pi}$ is $(\gamma_{2,1}, \gamma_{2,2})$- ordinary then for $c_3 > 4h_2\varepsilon^{-1}\kappa^{-1/2}$ we have

$$\lambda_2\left(\sigma_P\right) \le 2^4 h_2^2\varepsilon^{-2}Q^{-1}|b_2|^{-2} < \kappa c_3^2\, Q^{-2s} = \kappa\, \lambda_2\left(\overline{\Pi}\right).$$

Then we can write the following estimate for the measure of the set L':

$$\lambda_2\left(L'\right) \le \sum_{P \in \mathcal{P}_2(Q)} \lambda_2\left(\sigma_P\right) \le 2^4 h_2^2\varepsilon^{-2}Q^{-1} \sum_{\substack{b_2, b_1, b_0 \le Q: \\ P(t) = b_2t^2 + b_1t + b_0 \\ \sigma_P \ne \emptyset}} |b_2|^{-2}.$$

Let us estimate the number of polynomials $P \in \mathcal{P}_2(Q)$ having fixed leading coefficient and satisfying the inequalities (3.2.82) at some point $\mathbf{x} \in \overline{\Pi}$.

Consider the value of polynomial P at the points d_1, d_2. From Taylor expansions and estimates (3.2.83) we have

$$|P(d_i)| \le |P(x_i)| + c_{18}\,|b_2|\lambda_1\left(I_i\right), \tag{3.2.85}$$

for $Q > Q_0$. Consider a system of equations

$$\begin{cases} b_2 d_1^2 + b_1 d_1 + b_0 = l_1, \\ b_2 d_2^2 + b_1 d_2 + b_0 = l_2, \end{cases} \tag{3.2.86}$$

in three variables $b_2, b_1, b_0 \in \mathbb{Z}$, where $|l_i| \le 2c_{18} \max(1, |b_2|\lambda_1(I_i))$, $i = 1, 2$.

Let us estimate the number of possible solutions of (3.2.86) for a fixed b_2. Assume that for chosen b_2 there exists at least one solution $(b_2, b_{1,1}, b_{1,0})$ and consider the system (3.2.86) for two different triples $(b_2, b_{1,1}, b_{1,0})$ and $(b_2, b_{2,1}, b_{2,0})$. Simple transformations lead to the following system of linear equations in two variables $\tilde{b}_1 := b_{1,1} - b_{2,1}$ and $\tilde{b}_0 := b_{1,0} - b_{2,0}$

$$\begin{cases} \tilde{b}_1 d_1 + \tilde{b}_0 = l_{0,1} - l_{j,1}, \\ \tilde{b}_1 d_2 + \tilde{b}_0 = l_{0,2} - l_{j,2}. \end{cases} \tag{3.2.87}$$

Applying Lemma 3.2.5 with $K_i = 4c_{18} \max(1, |b_2|\lambda_1(I_i))$ we derive the following estimate for a fixed value of the coefficient b_2

$$\#(b_1, b_0) \le \begin{cases} 2^{10} c_{18}^2 \varepsilon^{-2} |b_2|^2 \lambda_2(\overline{\Pi}), & |b_2| > c_3^{-1} Q^s, \\ 2^{10} c_{18}^2 \varepsilon^{-2}, & Q^{s-\frac{1}{2}} < |b_2| < c_3^{-1} Q^s. \end{cases} \tag{3.2.88}$$

Let us consider the following two sets

$$L_1' = \bigcup_{\substack{P \in \mathcal{P}_2(Q), \\ c_3^{-1} Q^s < |b_2| < 4\delta_2 \varepsilon^{-1} Q}} \sigma_P, \qquad L_2' = \bigcup_{\substack{P \in \mathcal{P}_2(Q), \\ Q^{s-\frac{1}{2}} < |b_2| < c_3^{-1} Q^s}} \sigma_P.$$

The set L_1': In this case for $\delta_2 < 2^{-19} \kappa^{-1} c_{18}^{-2} h_2^{-2} \varepsilon^5$ we have

$$\lambda_2(L_1') \le 2^{14} c_{18}^2 h_2^2 \varepsilon^{-4} Q^{-1} \cdot 4\delta_2 \varepsilon^{-1} Q \lambda_2(\overline{\Pi}) < \tfrac{\kappa}{2} \lambda_2(\overline{\Pi}).$$

The set L_2': Consider the polynomials P under condition $Q^{s-\frac{1}{2}} < |b_2| < c_3^{-1} Q^s$. For every set σ_P we define the expanded set

$$\sigma_P' := \left\{ \mathbf{x} \in \overline{\Pi} : \quad |x_i - \alpha_i| < 4h_2 \varepsilon^{-1} \kappa^{-1/2} Q^{-\gamma_{2,i}} |b_2|^{-1}, i = 1, 2 \right\}. \tag{3.2.89}$$

Let us prove that for $|b_2| < c_{19} Q^{\frac{1}{2}}$, where $c_{19} = \frac{1}{18} \varepsilon \kappa^{1/2} h_2^{-1} (|d_1| + |d_2|)^{-1}$ those sets do not intersect.

Consider polynomials P_j, $j = 1, 2$ with roots $\alpha_{j,1}, \alpha_{j,2}$ and leading coefficients $|b_{j,2}| < c_{19} Q^{\frac{1}{2}}$. Without loss of generality we will assume $|b_{1,2}| < |b_{2,2}|$. Let there exists a point $\mathbf{x}_0 \in (\sigma_{P_1}' \cap \sigma_{P_2}')$. Since P_1 and P_2 have no common roots, the resultant $R(P_1, P_2)$ does not vanish, and the following estimate holds

$$1 = |b_{1,2}|^2 |b_{2,2}|^2 |\alpha_{1,1} - \alpha_{2,1}||\alpha_{1,1} - \alpha_{2,2}||\alpha_{1,2} - \alpha_{2,1}||\alpha_{1,2} - \alpha_{2,2}|. \tag{3.2.90}$$

By the estimates (3.2.89) we have

$$|\alpha_{1,i}-\alpha_{2,i}|\le|\alpha_{1,i}-x_{0,i}|+|\alpha_{2,i}-x_{0,i}|<2c_{19}\,Q^{-\gamma_{2,i}}|b_{1,2}|^{-1}.$$

On the other hand for $Q>Q_0$ we get

$$\begin{aligned}|\alpha_{1,1}-\alpha_{2,2}|&\le|\alpha_{1,1}|+|\alpha_{2,2}|\le\tfrac{3}{2}\,(|d_1|+|d_2|)\,,\\ |\alpha_{1,2}-\alpha_{2,1}|&\le|\alpha_{1,2}|+|\alpha_{2,1}|\le\tfrac{3}{2}\,(|d_1|+|d_2|)\,.\end{aligned}$$

By substituting these inequalities into (3.2.90) we obtain

$$1\le|R(P_1,P_2)|<36h_2^2\varepsilon^{-2}\kappa^{-1}\,(|d_1|+|d_2|)^2\,|b_{2,2}|^2\,Q^{-1}<\tfrac{1}{4}.$$

This contradiction yields the following estimate

$$\sum_{\substack{P\in\mathcal{P}_2(Q),\\ Q^{s-\frac12}<|b_2|<c_{19}\,Q^{\frac12}}}\lambda_2\left(\sigma_P\right)\le\tfrac{\kappa}{4}\sum_{\substack{P\in\mathcal{P}_2(Q),\\ Q^{s-\frac12}<|b_2|<c_{19}\,Q^{\frac12}}}\lambda_2\left(\sigma'_P\right)\le\tfrac{\kappa}{8}\,\lambda_2\left(\overline{\Pi}\right).$$

Consider the case $|b_2|>c_{19}\,Q^{\frac12}$. Denote by $\mathcal{P}_2(Q,k)\subset\mathcal{P}_2(Q)$, $1\le k\le K:=\left[\ln_2\left(\frac{2-2s}{3-4s}\right)\right]+1$ a subclass of polynomials defined as follows

$$\mathcal{P}_2(Q,k):=\left\{P\in\mathcal{P}_2(Q):l_{k+1}\,Q^{\lambda_{k+1}}\le|b_2|\le l_k\,Q^{\lambda_k}\right\},$$

where

$$\begin{aligned}&\lambda_1=s, && l_1=c_3^{-1},\\ &\lambda_k=\lambda_{k-1}-(1-s)\,2^{1-k}, && l_k=\frac{2^8c_{18}h_2\sqrt{K\,l_{k-1}}}{\sqrt{\kappa}\varepsilon^2c_3}\quad\text{for } 2\le k\le K,\\ &\lambda_{K+1}=\tfrac12, && l_{K+1}=c_{19}.\end{aligned}$$

These equations give $\lambda_k=s-(1-s)\,\left(1-\frac{1}{2^{k-1}}\right)$ for $2\le k\le K$.

Let us consider the following sets $L(k):=\bigcup\limits_{P\in\mathcal{P}_2(Q,k)}\sigma_P$ and estimate the measure of every set as follows

$$\begin{aligned}\lambda_2\left(L(k)\right)=\sum_{P\in\mathcal{P}_2(Q,k)}\lambda_2\left(\sigma_P\right)&\le\frac{2^{14}h_2^2c_{18}^2}{\varepsilon^4}\,Q^{-1}\sum_{l_{k+1}Q^{\lambda_{k+1}}\le|b_2|\le l_kQ^{\lambda_k}}|b_2|^{-2}\\ &\le\frac{2^{14}h_2^2c_{18}^2l_k}{\varepsilon^4l_{k+1}^2}\,Q^{-1-2\lambda_{k+1}+\lambda_k}.\end{aligned}$$

Then for $k=1$ we obtain

$$\lambda_2\left(L(1)\right)\le\tfrac{c_3^2\kappa}{4K}\,Q^{-1-2s+1-s+s}\le\tfrac{\kappa}{4K}\,c_3^2Q^{-2s}<\tfrac{\kappa}{4K}\,\lambda_2\left(\overline{\Pi}\right);$$

for $1<k\le K-1$ we have

$$\lambda_2\left(L(k)\right)\le\tfrac{c_3^2\kappa}{4K}\,Q^{-1+s-(1-s)\left(1-\frac{1}{2^{k-1}}\right)-2s+(1-s)\left(2-\frac{1}{2^{k-1}}\right)}\le\tfrac{\kappa}{4K}\,c_3^2Q^{-2s}=\tfrac{\kappa}{4K}\,\lambda_2\left(\overline{\Pi}\right);$$

and for $k = K$, $s < \frac{3}{4}$ and $Q > Q_0$ we get

$$\lambda_2\left(L(K)\right) \le \frac{2^{14}h_2^2c_{18}^2\,l_K}{\varepsilon^4 c_{19}^2}\,Q^{-2+s-(1-s)\left(1-\frac{1}{2^{K-1}}\right)} \le \frac{2^{14}h_2^2c_{18}^2\,l_K}{\varepsilon^4 c_{19}^2}\,Q^{-3+2s+(1-s)\frac{3-4s}{2-2s}}$$
$$\le \frac{2^{14}h_2^2c_{18}^2\,l_K}{\varepsilon^4 c_{19}^2}\,Q^{-\frac{3}{2}} < \frac{\kappa}{4K}\,\lambda_2\left(\overline{\Pi}\right).$$

Then, we obtain following estimate for the measure of the set L_2'

$$\lambda_2\left(L_2'\right) \le \sum_{\substack{P\in\mathcal{P}_2(Q),\\ Q^{s-\frac{1}{2}}<|b_2|<c_{19}\,Q^{\frac{1}{2}}}} \lambda_2\left(\sigma_P\right) + \sum_{1\le k\le K} \lambda_2\left(L(k)\right) \le \tfrac{\kappa}{2}\,\lambda_2\left(\overline{\Pi}\right),$$

and, thus,

$$\lambda_2\left(L'\right) \le \lambda_2\left(L_1'\right) + \lambda_2\left(L_2'\right) \le \kappa\,\lambda_2\left(\overline{\Pi}\right).$$

Now the proof of Lemma 3.2.8 can be finished by repeating the proof of Lemma 3.2.6. □

Theorem 3.2.2 can be proved by applying the results of Lemma 3.2.8 to the proof of Theorem 3.2.1.

3.2.4 Proof of Theorem 3.2.3: Upper Bound

Assume the converse. Let

$$\mathcal{N}_n^2(\mathbb{A}, Q, \Pi) \ge c_6\,Q^{n+1}\lambda_2\left(\Pi\right)$$

and consider a point $\boldsymbol{\alpha}$ with algebraic conjugate coordinates $\alpha_1, \alpha_2 \in \mathbb{A}_{n,H}(Q) \cap \Pi$. Let P be a minimal polynomial of algebraic numbers α_1 and α_2 and let us derive an estimate for the polynomial P at points d_1, d_2. Since $\alpha_i \in I_i$ then by Lemma 3.2.4 we have

$$|P^{(k)}(\alpha_i)| \le \tfrac{n!}{(n-k)!}\,\omega_{n-k+1}(3/2\,d_i)\,Q,$$

for all $1 \le k \le n$ and $Q > Q_0$. From these estimates and a Taylor expansion of P in the intervals I_i, $i = 1, 2$ we obtain the following inequalities

$$|P(d_i)| \le \sum_{k=1}^{n} \left|\tfrac{1}{k!}P^{(k)}(\alpha_i)(d_i-\alpha_i)^k\right| \le 2^n\omega_n(3/2\,d_i)\,Q\lambda_1\left(I_i\right). \tag{3.2.91}$$

Let us fix a vector $\mathbf{a} := (a_n, \ldots, a_2) \in \mathbb{Z}^{n-1}$ and denote by $\mathcal{P}_n(Q, \mathbf{a}) \subset \mathcal{P}_n(Q)$ the following subclass of polynomials

$$\mathcal{P}_n(Q, \mathbf{a}) := \left\{P \in \mathcal{P}_n(Q)\colon P(t) = a_n t^n + \ldots + a_2 t^2 + a_1 t + a_0 \text{ satisfies } (3.2.91)\right\}$$

having the same vector of coefficients $\mathbf{a}$ and satisfying (3.2.91). The number of non-empty subclasses $\mathcal{P}_n(Q, \mathbf{a})$ is bounded by the number of vectors $\mathbf{a}$ lying inside the box $[-Q; Q]^{n-1}$, which can be estimated as follows

$$\#\left([-Q; Q]^{n-1} \cap \mathbb{Z}^{n-1}\right) = (2Q+1)^{n-1} < 2^n\,Q^{n-1} \tag{3.2.92}$$

for $Q > Q_0$. It should also be noted that every point with algebraic conjugate coordinates from the set $\mathbb{A}_n(Q) \cap \Pi$ corresponds to a polynomial $P \in \mathcal{P}_n(Q)$ that satisfies (3.2.91). On the other hand, every polynomial $P \in \mathcal{P}_n(Q)$ satisfying (3.2.91) corresponds to at most n^2 such points. This allows us to write

$$c_6\, Q^{n+1}\lambda_2\left(\Pi\right) < \mathcal{N}_n^2(\mathbb{A}, Q, \Pi) \le n^2 \sum_{\mathbf{a}} \#\mathcal{P}_n(Q, \mathbf{a}).$$

Thus, by the estimate (3.2.92) and pigeonhole principle applied to the vectors $\mathbf{a}$ and polynomials P satisfying (3.2.91), there exists a vector $\mathbf{a}_0$ such that

$$\#\mathcal{P}_n(Q, \mathbf{a}_0) \ge c_6\, 2^{-n} n^{-2} Q^2 \lambda_2\left(\Pi\right). \tag{3.2.93}$$

Let us find an upper bound for the value $\#\mathcal{P}_n(Q, \mathbf{a}_0)$. In order to do this, we fix some polynomial $P_0 \in \mathcal{P}_n(Q, \mathbf{a}_0)$ and consider the difference between the polynomials P_0 and $P_j \in \mathcal{P}_n(Q, \mathbf{a}_0)$ at points d_i, $i = 1, 2$. From the estimate (3.2.91) it follows

$$|P_0(d_i) - P_j(d_i)| = |(a_{0,1} - a_{j,1})d_i + (a_{0,0} - a_{j,0})| \le 2^{n+1}\omega_n(3/2\, d_i)\, Q\lambda_1\left(I_i\right).$$

Thus, the number of different polynomials $P_j \in \mathcal{P}_n(Q, \mathbf{a}_0)$ does not exceed the number of integer solutions of the following system

$$|b_1 d_i + b_0| \le 2^{n+1}\omega_n(3/2\, d_i)\, Q\lambda_1\left(I\right)_i, \quad i = 1, 2.$$

Now let us apply Lemma 3.2.5 with $K_i = 2^{n+1}\omega_n(3/2\, d_i)\, Q\lambda_1\left(I_i\right)$. Since $\lambda_1\left(I_i\right) = c_5 Q^{-s_i}$ and $s_i < 1$, we have $K_i \ge 2^{n+1}\omega_n(3/2\, d_i) c_5\, Q^{1-s_i} > \max\left(|d_1 - d_2|, 1\right)$ for $Q > Q_0$. This implies that

$$\#\mathcal{P}_n(Q, \mathbf{a}_0) \le 2^{2n+8}|d_1 - d_2|^{-1}\omega_n(3/2\, d_1)\omega_n(3/2\, d_2)\, Q^2\lambda_2\left(\Pi\right),$$

which contradicts to inequality (3.2.93) for $c_6 = 2^{3n+9} n^2 \omega_n(3/2\, d_1)\omega_n(3/2\, d_2)|d_1 - d_2|^{-1}$. Thus,

$$\mathcal{N}_n^2(\mathbb{A}, Q, \Pi) < c_6\, Q^{n+1}\lambda_2\left(\Pi\right).$$

3.3 Neighborhood of Curves

One of the interesting and important topic is the distribution of points with rational coordinates near curves. Let $f : J_0 \to \mathbb{R}$ be a $C^2(J_0)$ function defined on a finite open interval $J_0 \subset \mathbb{R}$. Suppose also that there exist constants C_2, C_3 with $0 < C_2 \le C_3 < \infty$ such that

$$C_2 \le |f''(x)| \le C_3$$

for all $x \in J_0$. We will denote the class of such functions by $\mathcal{F}(C_2, C_3, J_0)$. Consider the following set

$$N_f(Q, \lambda, J) := \#\left\{\left(\frac{p_1}{q}, \frac{p_2}{q}\right) \in \mathbb{Q}^2 : 0 < q \le Q,\ \frac{p_1}{q} \in J,\ \left|f\left(\frac{p_1}{q}\right) - \frac{p_2}{q}\right| < Q^{-\lambda}\right\},$$

where $J \subset J_0$ and $0 \leq \lambda < 2$. In other words, the quantity $N_f(Q, \lambda, J)$ denotes the number of rational points with bounded denominators lying within a certain neighborhood of the curve parametrized by f. The problem is to find the asymptotics for $N_f(Q, \lambda, J)$ as $Q \to \infty$.

The next results are formulated for functions $f \in \mathcal{F}(C_2, C_3, J_0)$. The first step in solving the problem above has been made by Huxley in [41], where he proved the following upper estimate for any $\varepsilon > 0$

$$N_f(Q, \lambda, J) \ll Q^{3-\lambda+\epsilon}.$$

An estimate without ε in the exponent has been obtained in 2006 in paper of Vaughan and Velani [64]. They showed that

$$N_f(Q, \lambda, J) \ll Q^{3-\lambda} + Q^{\frac{1}{2}+\frac{\lambda}{2}},$$

and, moreover, under the additional condition that f has Lipschitz continuous second derivative with Lipschitz constant $\theta \in (0, 1)$ we have

$$N_f(Q, \lambda, J) \ll Q^{3-\lambda} + Q^{1-\frac{\lambda(\theta-1)}{2}},$$

where the constants in the Vinogradov symbol depend on C_2, C_3 and the measure of the interval J only. It should be noted that for $\lambda \leq \frac{5}{3}$, the estimate of Vaughan and Velani is indeed better than the estimate of Huxley for an arbitrary function $f \in \mathcal{F}(C_2, C_3, J_0)$, but for $\lambda > \frac{5}{3}$ only functions having a Lipschitz continuous second derivative with Lipschitz constant $\theta \leq 3 - \frac{4}{\lambda}$ give the best possible upper bound $\ll Q^{3-\lambda}$. The lower estimate of the same order was obtained by Beresnevich, Dickinson and Velani [8] for any function $f \in C^3(J_0)$.

3.3.1 Main Result

Since the set of rational numbers with denominator at most Q is basically the set of algebraic numbers of first degree and 'naïve' height at most Q, we can formulate the problem above in a more general setup, namely for the set of points with algebraic conjugate coordinates. Let $f : J_0 \to \mathbb{R}$ be a continuously differentiable function defined on a finite open interval $J_0 \subset \mathbb{R}$ and satisfying the conditions:

$$\sup_{x \in J_0} |f'(x)| := c_{20} < \infty, \qquad \#\{x \in J_0 : f(x) = x\} < \infty. \tag{3.3.1}$$

Denote by $L_f^n(Q, \lambda, J)$ the following set

$$L_{\lambda,J}^f = L_{\lambda,J}^f(Q) := \left\{ \mathbf{x} \in \mathbb{R}^2 : |x_2 - f(x_1)| < \left(\tfrac{1}{2} + c_{20}\right) c_{21}\, Q^{-\lambda}, \quad x_1 \in J \right\}, \tag{3.3.2}$$

where $J \subseteq J_0$. The problem reduces to counting points with algebraic conjugate coordinates in specific domain $L_{\lambda,J}^f$. A few years ago, Bernik, Götze, and Kukso [13] obtained the following lower bound

$$\mathcal{N}_n^2\left(\mathbb{A}, Q, L_{\lambda,J}^f\right) \gg Q^{n+1-\lambda}$$

for $0 < \lambda < \frac{1}{2}$, $Q > Q_0$, where the constants in the Vinogradov symbol and the value Q_0 depend on n, λ, the function f and the length of the interval J only.

We will improve on this result to obtain an identical estimate for $0 < \lambda < \frac{3}{4}$ and derive the upper bound of the same order.

Theorem 3.3.1. *Let $f : J_0 \to \mathbb{R}$ be a continuously differentiable function defined on a finite open interval $J_0 \subset \mathbb{R}$ and satisfying the conditions (3.3.1). Let $L^f_{\lambda,J}$ be the set defined by (3.3.2). Then for any $0 < \lambda < \frac{3}{4}$, integer $n \geq 2$, $c_{21} > c_0(n, \lambda, J, f)$ and positive $Q > Q_0(J, f, n, \lambda)$ there exists the positive values c_{22}, c_{23} depending on J, f, and n only, such that*

$$c_{22}\, Q^{n+1-\lambda} \leq \mathcal{N}^2_n\left(\mathbb{A}, Q, L^f_{\lambda,J}\right) \leq c_{23}\, Q^{n+1-\lambda}.$$

To prove Theorem 3.3.1 we are going to use the results of Theorem 3.2.1, Theorem 3.2.2 and Theorem 3.2.3.

Note that the distance between algebraically conjugate numbers is bounded from below [18, 28], meaning that a certain neighborhood of the line $y = x$ must be excluded from consideration. For this purpose let us consider the set $D_0 := \left\{x \in J : |f(x) - x| < \frac{\varepsilon}{2}\right\}$, where $\varepsilon > 0$ is a small positive constant. Since the number of points $x \in J$ such that $f(x) = x$ is finite, for a sufficiently small constant ε we have that $\lambda_1(D_0) < \frac{1}{4}\lambda_1(J)$.

3.3.2 Proof: Lower Bound

Instead of the interval J, let us consider the set $J \setminus D_0 = \bigcup\limits_k J_k$. Due to condition (3.3.1) the number of intervals J_k is finite and

$$\lambda_2(J \setminus D_0) \geq \tfrac{3}{4}\lambda_1(J). \tag{3.3.3}$$

Now for every strip $L^f_{\lambda,J_k}(Q)$ we have $L^f_{\lambda,J_k}(Q) \cap \left\{\mathbf{x} \in \mathbb{R}^2 : |x_1 - x_2| < \varepsilon\right\} = \emptyset$.

For every interval $J_k = [b_{k,1}, b_{k,2}]$ consider the strip $L^f_{\lambda,J_k}(Q)$ and estimate the cardinality of the set $\mathcal{N}^2_n\left(\mathbb{A}, Q, L^f_{\lambda,J_k}\right)$ for a fixed $0 < \lambda < \frac{3}{4}$. Let us divide the strip $L^f_{\lambda,J_k}(Q)$ into subsets

$$E_j := \left\{\mathbf{x} \in \mathbb{R}^2 : x_1 \in J_{k,j}, |x_2 - f(x_1)| < \left(\tfrac{1}{2} + c_{20}\right) c_3\, Q^{-\lambda}\right\},$$

where $J_{k,j} = [y_j, y_{j+1}]$, $y_0 = b_{k,1}$ and $y_j = y_{j-1} + c_{21}\, Q^{-\lambda}$. The number t_k of subsets E_j for $Q > Q_0$ can be estimated as follows

$$t_k \geq \frac{\lambda_1(J_k)}{\lambda_1(J_{k,j})} - 1 > \tfrac{1}{2}\, c_{21}^{-1}\, Q^{\lambda}\, \lambda_1(J_k). \tag{3.3.4}$$

Define $\overline{f}_j := \frac{1}{2}\left(\max\limits_{x \in J_{k,j}} f(x) + \min\limits_{x \in J_{k,j}} f(x)\right)$ and consider the rectangles

$$\Pi_j := \left\{\mathbf{x} \in \mathbb{R}^2 : x_1 \in J_{k,j}, \left|x_2 - \overline{f}_j\right| \leq \tfrac{1}{2} c_3\, Q^{-\lambda}\right\}.$$

Since f is continuous and differentiable function on every interval $J_{k,j}$ and $\sup\limits_{x\in J_{k,j}}|f'(x)|\le\sup\limits_{x\in J}|f'(x)|=c_{20}$ by the mean value theorem we have

$$\left|\max_{x\in J_{k,j}}f(x)-\min_{x\in J_{k,j}}f(x)\right|\le|f'(\xi)|\,\lambda_1\left(J_{k,j}\right)<c_{20}c_{21}\,Q^{-\lambda},$$

which means that $\Pi_j\subset E_j$ for every $1\le j\le t_k$. Thus, every set E_j corresponds to the square $\Pi_j=I_{j,1}\times I_{j,2}$ of size $\lambda_2\left(\Pi_j\right)=c_{21}^2Q^{-2\lambda}$.

Case 1: $0<\lambda\le\frac{1}{2}$.

In this case, we apply the result of Theorem 3.2.1 to every square Π_j to derive the estimate

$$\mathcal{N}_n^2\left(\mathbb{A},Q,\Pi_j\right)\ge c_2\,Q^{n+1}\lambda_2\left(\Pi_j\right)=c_2c_{21}^2\,Q^{n+1-2\lambda},$$

for $Q>Q_0$ and c_{21} being sufficiently large. Using (3.3.3) and (3.3.4) we have

$$\begin{aligned}\mathcal{N}_n^2\left(\mathbb{A},Q,L^f_{\lambda,J}\right)&\ge\sum_k\sum_{j=1}^{t_k}\mathcal{N}_n^2\left(\mathbb{A},Q,\Pi_j\right)\ge\tfrac{1}{2}c_2c_{21}\,Q^{n+1-\lambda}\sum_k\lambda_1\left(J_k\right)\\&\ge\tfrac{3}{8}c_2c_{21}\lambda_1\left(J\right)\,Q^{n+1-\lambda}=c_{22}\,Q^{n+1-\lambda}.\end{aligned}$$

Case 2: $\frac{1}{2}<\lambda<\frac{3}{4}$.

In this case we need to apply Theorem 3.2.2. Let us estimate the number of $\left(\frac{1}{2},\frac{1}{2}\right)$-special squares Π_j. By the definition, $\left(\frac{1}{2},\frac{1}{2}\right)$- special square contains the points $\mathbf{x}_0$ such that there exists a polynomial $P\in\mathcal{P}_2(Q)$ with leading coefficient b_2 satisfying the inequalities

$$\begin{cases}|P(x_{0,i})|<h_2\,Q^{-\frac{1}{2}},\quad i=1,2,\\|b_2|\le Q^{\lambda-\frac{1}{2}}.\end{cases}\tag{3.3.5}$$

Repeating the steps of the proof from the beginning of Subsection 3.2.2.1 we obtain the following estimates

$$|P'(\alpha_1)|=|P'(\alpha_2)|>\tfrac{3}{4}\,\varepsilon\,|b_2|.$$

Thus, by Lemma A.1.14 the set of points $\mathbf{x}$ satisfying (3.3.5) for a fixed polynomial P is a subset of the following square

$$\sigma_P:=\left\{\mathbf{x}\in\mathbb{R}^2:|x_i-\alpha_i|\le2h_2\varepsilon^{-1}\,Q^{-\frac{1}{2}}|b_2|^{-1},i=1,2\right\}.$$

Let us estimate the number of squares Π_j, such that $\Pi_j\cap\sigma_P\ne\emptyset$. It is easy to see that the width of the strip $L_f(Q,\lambda,J_k)$ is smaller than the height of the square σ_P for sufficiently large c_{21}. Hence, every σ_P intersects with at most $4h_2\varepsilon^{-1}c_{21}^{-1}\,Q^{\lambda-\frac{1}{2}}|b_2|^{-1}$ squares Π_j. Therefore, the number m_1 of $\left(\frac{1}{2},\frac{1}{2}\right)$- special squares Π_i can be estimated as follows

$$m_1\le\sum_{P\in\mathcal{P}_2(Q)}4h_2\varepsilon^{-1}c_{21}^{-1}\,Q^{\lambda-\frac{1}{2}}|b_2|^{-1}\le4h_2\varepsilon^{-1}c_{21}^{-1}\,Q^{\lambda-\frac{1}{2}}\sum_{b_2,b_1,b_0}|b_2|^{-1}$$

Now we need to estimate the number of polynomials $P \in \mathcal{P}_2(Q)$ having leading coefficient b_2 and satisfying the inequalities (3.3.5) at some point $\mathbf{x} \in L_f(Q, \lambda, J_k)$. Since the function f is continuously differentiable on the interval J and $\sup\limits_{x \in J_k} |f'(x)| < c_{20}$, by the mean value theorem we get

$$\left| \max_{x \in J_k} f(x) - \min_{x \in J_k} f(x) \right| < c_{20}\, \lambda_1 (J_k)\,,$$

which implies that the set $L_f(Q, \lambda, J_k)$ belongs to a rectangle $\Pi = I_1 \times I_2$, where $\lambda_1 (I_2) = c_{20}\, \lambda_1 (I_1) = c_{20} \lambda_1 (J_k)$.

Let us estimate the value of the polynomial P at the middle point $\mathbf{d}$ of the rectangle Π. Using the arguments from the beginning of Subsection 3.2.2.1 we obtain

$$|P(d_1)| \le c_{24}\, |b_2| \lambda_1 (J_k)\,, \quad |P(d_2)| \le c_{24} c_{20}\, |b_2| \lambda_1 (J_k)\,.$$

and, hence, for a fixed value of b_2 the number of polynomials $P \in \mathcal{P}_2(Q)$ satisfying the inequalities (3.3.5) at some point $\mathbf{x} \in \Pi$ can be estimated as follows

$$\#(b_1, b_0) \le 2^5 c_{20} c_{24}^2 \varepsilon^{-1} |b_2|^2 \left(\lambda_1 (J_k)\right)^2 .$$

Using this estimate we obtain

$$\begin{aligned} m_1 &\le 2^7 h_2 c_{20} c_{24}^2 c_{21}^{-1} \varepsilon^{-3} \left(\lambda_1 (J_k)\right)^2 Q^{\lambda - \frac{1}{2}} \sum_{|b_2| < Q^{\lambda - \frac{1}{2}}} |b_2| \\ &\le 2^7 h_2 c_{20} c_{24}^2 c_{21}^{-1} \varepsilon^{-3} \left(\lambda_1 (J_k)\right)^2 Q^{3\lambda - \frac{3}{2}} \\ &< \frac{1}{4} c_{21}^{-1} \lambda_1 (J_k)\, Q^{\lambda} < \tfrac{t_k}{2}. \end{aligned} \tag{3.3.6}$$

for $\lambda < \frac{3}{4}$ and $Q > Q_0$. By (3.3.6), it follows that the number of $\left(\frac{1}{2}, \frac{1}{2}\right)$-ordinary squares Π_j does not exceed

$$m_2 \ge t_k - \tfrac{1}{2} t_k > \tfrac{1}{2} t_k. \tag{3.3.7}$$

From Theorem 3.2.2 and the estimate (3.3.7) we obtain

$$\begin{aligned} \mathcal{N}_n^2 \left(\mathbb{A}, Q, L_{\lambda, J}^f\right) &\ge \sum_k \sum_{\substack{\Pi_j \in L_f(Q, \lambda, J_k) \\ \Pi_j - \left(\frac{1}{2}, \frac{1}{2}\right)\text{-special}}} \mathcal{N}_n^2 (\mathbb{A}, Q, \Pi_j) \ge \tfrac{1}{4} c_4 c_{21}\, Q^{n+1-\lambda} \sum_k \lambda_1 (J_k) \\ &\ge \tfrac{3}{16} c_4 c_{21} \lambda_1 (J)\, Q^{n+1-\lambda} = c_{22}\, Q^{n+1-\lambda}. \end{aligned}$$

3.3.3 Proof: Upper Bound

In the same way as in the previous section, let us divide the set $L_{\lambda, J}^f(Q)$, $J = [b_1, b_2]$ into subsets

$$E_j := \left\{ \mathbf{x} \in \mathbb{R}^2 : x_1 \in J_j, |f(x_1) - x_2| < \left(\tfrac{1}{2} + c_{20}\right) c_{21}\, Q^{-\lambda} \right\},$$

where $J_j = [y_{j-1}, y_j]$, $y_0 = b_1$, $y_{j+1} = y_j + \left(\frac{1}{2} + \frac{3}{2}c_{20}\right) c_{21}\, Q^{-\lambda}$ and the number t of subsets E_j satisfies the inequality

$$t \le \frac{\lambda_1(J)}{\lambda_1(J_j)} \le \left(\tfrac{1}{2} + \tfrac{3}{2}c_{20}\right)^{-1} c_{21}^{-1}\, Q^{\lambda}\, \lambda_1(J). \tag{3.3.8}$$

Define $\overline{f}_j := \frac{1}{2}\left(\max\limits_{x\in J_j} f(x) + \min\limits_{x\in J_j} f(x)\right)$ and consider the squares

$$\Pi_j := \left\{\mathbf{x} \in \mathbb{R}^2 : x_1 \in J_j, \left|\overline{f}_j - x_2\right| < \left(\tfrac{1}{2} + \tfrac{3}{2}c_{20}\right) c_{21}\, Q^{-\lambda}\right\}.$$

Since the function f is continuously differentiable on the interval J, and $\max\limits_{x\in J} |f'(x)| = c_{20}$, it is easy to see that $E_j \subset \Pi_j$, $1 \le j \le t$.

Note that the squares Π_j satisfy the conditions of Theorem 3.2.3. Therefore

$$\mathcal{N}_n^2(\mathbb{A}, Q, \Pi_j) \le c_6\, Q^{n+1} \lambda_2(\Pi_j) = c_6 c_3^2 \left(\tfrac{1}{2} + \tfrac{3}{2}c_{20}\right)^2 Q^{n+1-2\lambda}.$$

These inequalities, together with the estimate (3.3.8), lead to the following

$$\mathcal{N}_n^2\left(\mathbb{A}, Q, L^f_{\lambda,J}\right) \le c_6 c_{21} \left(\tfrac{1}{2} + \tfrac{3}{2}c_{20}\right) \lambda_1(J)\, Q^{n+1-\lambda} = c_{23}\, Q^{n+1-\lambda}.$$

3.4 Distribution of Algebraic Integers and Points with Conjugate Algebraic Integer Coordinates

In this section we investigate the distribution of algebraic integers on the real line and the distribution of the points with algebraic conjugate integer coordinates in the Euclidean plane. We will consider the same problem as in the previous sections formulated for algebraic integers.

The first part of this section is devoted to the study of one-dimensional case, namely algebraic integers. Given an interval $I \subset \mathbb{R}$, denote by $\mathcal{N}_n(\mathcal{O}, Q, I)$ the number of algebraic integers $\alpha \in I$ of degree n and 'naïve' height at most Q. We will prove the following theorem.

Theorem 3.4.1. *For any interval I of length $\lambda_1(I) = c_{25}\, Q^{-s}$, $0 < s \le 1$ with middle point d, any integer $n \ge 2$, positive real $Q > Q_0(n, d, s)$, and $c_{25} > c_0(n, d) > 0$ there exist positive constants c_{26}, c_{27} depending on n and d only, such that*

$$c_{27} Q^n\, \lambda_1(I) \ge \mathcal{N}_n(\mathcal{O}, Q, I) \ge c_{26} Q^n\, \lambda_1(I).$$

Remark 3.4.2. *It should be noted that the condition $s \le 1$ can not be omitted. As was mentioned above there exist intervals of length $\asymp Q^{-1}$ which do not contain algebraic numbers from the set $\mathbb{A}_n(Q)$. Since $\mathcal{O}_n(Q) \subset \mathbb{A}_n(Q)$ the same statement holds for algebraic integers.*

Another way to formulate Theorem 3.4.1 is to say that the set of real algebraic integers of degree n forms a regular system and from the proof of Theorem 3.4.1 one can immediately derive the following corollary.

Corollary 3.4.2.1. *The set of algebraic integers $\mathcal{O}_n$ together with function $N_3(\alpha) = H(\alpha)^n (1 + |\alpha|)^{n(n-1)}$ is a regular system with parameter $T_0(\mathcal{O}_n, N_3, I) = C(n) (\lambda_1 (I))^{-n}$.*

In the second part of this section we proceed with the study of two-dimensional analogue of Theorem 3.4.1. As in case of points with algebraic conjugate coordinates consider a rectangle $\Pi = I_1 \times I_2$ with middle point $\mathbf{d} = (d_1, d_2)$, $d_1 \neq d_2$ and sizes $\lambda_1 (I_1) = c_{1,1} Q^{-s_1}$, $\lambda_1 (I_2) = c_{1,2} Q^{-s_2}$, where $0 < s_1 + s_2 < 1$.

Theorem 3.4.3. *For any rectangle $\Pi = I_1 \times I_2$ with middle point $\mathbf{d} = (d_1, d_2)$, $d_1 \neq d_2$ satisfying the following conditions:*

1. *$\lambda_1 (I_i) = c_{1,i} Q^{-s_i}$, where $s_i < 1$ and $0 < s_1 + s_2 \leq 1$, $i = 1, 2$;*
2. *$c_{1,1} c_{1,2} > c_0(n, \mathbf{d}) > 0$ for $s_1 + s_2 = 1$;*

any integer $n \geq 3$, and any positive real $Q > Q_0(n, \mathbf{d}, \mathbf{s})$ there exists a constant $c_{28} = c_{28}(n, \mathbf{d}) > 0$, such that

$$\mathcal{N}_n^2 (\mathcal{O}, Q, \Pi) \geq c_{28} Q^n \lambda_2 (\Pi).$$

Theorem 3.4.4. *Let $\Pi = I_1 \times I_2$ be a rectangle with a middle point $\mathbf{d}$, $d_1 \neq d_2$ and sides $\lambda_1 (I_i) = c_5 Q^{-s_i}$, $i = 1, 2$. Then for any integern ≥ 3, any $0 < s_1, s_2 < 1$, and any positive real$Q > Q_0(n, \mathbf{s}, \mathbf{d})$ we have*

$$\mathcal{N}_n^2 (\mathcal{O}, Q, \Pi) < c_{29} Q^n \lambda_2 (\Pi),$$

where $c_{29} = 2^{3n+9} n^2 \omega_n(3/2\, d_1) \omega_n(3/2\, d_2) |d_1 - d_2|^{-1}$.

Proof. The proof of Theorem 3.4.4 is analogous to the proof of Theorem 3.2.3. □

The last result is analogue of Theorem 3.3.1.

Theorem 3.4.5. *Let $f : J_0 \to \mathbb{R}$ be a continuously differentiable function defined on a finite open interval $J_0 \subset \mathbb{R}$ and satisfying the conditions (3.3.1). Let $L^f_{\lambda,J}$ be the set defined by (3.3.2). Then for any $0 < \lambda < \frac{1}{2}$, any integer $n \geq 3$, and any positive real $Q > Q_0(J, f, n, \lambda)$ there exists the positive constants c_{30}, c_{31} depending on J, f and n only, such that*

$$c_{30} Q^{n-\lambda} \leq \mathcal{N}_n^2 \left(\mathcal{O}, Q, L^f_{\lambda,J}\right) \leq c_{31} Q^{n-\lambda}.$$

Proof. The proof of this Theorem is analogous to the proof of Theorem 3.3.1 using the result of Theorem 3.4.3 instead of the result of Theorem 3.2.1 and the result of Theorem 3.4.4 instead of the result of Theorem 3.2.3. □

3.4.1 Proof of Theorem 3.4.1

3.4.1.1 Lower Bound

The proof of the lower bound is based on the following lemma.

Lemma 3.4.6 (see [14]). *Let $I \subset \mathbb{R}$ be the interval of length $\lambda_1(I) = c_{32}\,Q^{-1}$, where $c_{32} > 0$. Denote by $L_n = L_n(Q, \delta, I)$ the set of points $x \in I$ such that there exists a polynomial $P \in \mathcal{P}_n(Q)$ satisfying the inequalities*

$$\begin{cases} |P(x)| < Q^{-n}, \\ |P'(x)| < \delta Q. \end{cases}$$

Then $\lambda_1(L_n) < \frac{1}{4}\lambda_1(I)$ for $\delta < \delta_0(n) > 0$, and $Q > Q_0(n)$.

Remark 3.4.7. *It suffices to take $\delta(n) = 2^{-n-8}n^{-2}$ (see [14] for more details).*

Remark 3.4.8. *One can also prove Lemma 3.4.6 in a bit more general form, namely for the intervals I of length $\lambda_1(I) = c_{32}\,Q^{-s}$, $0 < s \leq 1$ and for the system*

$$\begin{cases} |P(x)| < \hat{h}\,Q^{-n}, \\ |P'(x)| < \delta Q, \end{cases}$$

where $\hat{h}$ is some constant independent of Q. The proof in this case is the same as in the original statement and the only changes appear in the value of the constants δ_0, c_0 and Q_0. We will use this more general form of Lemma 3.4.6 in our proof.

Let $L^1 = L_{n-1}(Q, \delta, I)$ be the set of points $x \in I$ such that there exists a polynomial $P \in \mathcal{P}_{n-1}(Q)$ satisfying the inequalities

$$\begin{cases} |P(x)| < \hat{h}\,Q^{-n+1}, \\ |P'(x)| < \delta\,Q. \end{cases} \tag{3.4.1}$$

Applying Lemma 3.4.6 for $Q > Q_0$ and $\delta < \delta_0(n, d)$ we can estimate the measure of the set L^1 as follows

$$\lambda_1\left(L^1\right) \leq \tfrac{1}{4}\lambda_1(I).$$

Let us consider the set $B^1 := I \backslash L^1$. From the Minkowski's linear forms theorem (Lemma A.2.3) it follows that for every point $x \in I$ and $Q > Q_0$ there exists a non-zero polynomial $P(t) = a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \in \mathbb{Z}[t]$ satisfying

$$|P(x)| \leq \hat{h}\,Q^{-n+1}, \quad |a_j| \leq \tfrac{2}{3}\,d^{-1}\omega_n^{-1}(3/2d)\;Q \quad (1 \leq j \leq n-1),$$

where $\hat{h} = \left(3/2\,d\omega_n\left(\frac{3}{2}d\right)\right)^{n-1}$. One can easily verify that $|a_0| < Q$ and, hence, $P \in \mathcal{P}_{n-1}(Q)$. This means that for any $x_0 \in B^1$ and any polynomial $P \in \mathcal{P}_{n-1}(Q)$ we have

$$\begin{cases} |P(x_0)| < \hat{h}\,Q^{-n+1}, \\ |P'(x_0)| \geq \delta\,Q, \end{cases}$$

and, moreover, $\lambda_1\left(B^1\right) \geq \frac{3}{4}\lambda_1(I)$.

Consider an arbitrary point $x_0 \in B^1$ and examine successive minima $\tau_1, \ldots, \tau_n$ of the compact convex set K defined by inequalities

$$\begin{cases} |a_{n-1}x_0^{n-1} + \ldots + a_1 x_0 + a_0| \leq \hat{h}\,Q^{-n+1}, \\ |(n-1)a_{n-1}x_0^{n-2} + \ldots + 2a_2 x_0 + a_1| \leq Q, \\ |a_{n-1}|, \ldots, |a_2| \leq Q. \end{cases} \tag{3.4.2}$$

Assume, that $\tau_1 \leq \delta$. Then for δ being sufficiently small there exists a non-zero polynomial $P_0 \in \mathcal{P}_{n-1}(Q)$ satisfying the inequalities

$$\begin{cases} |P_0(x_0)| \leq \delta \hat{h}\, Q^{-n+1} < \hat{h}\, Q^{-n+1}, \\ |P_0'(x_0)| \leq \delta\, Q, \\ H(P_0) \leq Q, \end{cases}$$

which contradicts the fact that $x_0 \in B^1 = I \backslash L^1$. thus, we conclude that $\tau_{n-1} \geq \ldots \geq \tau_1 > \delta$. Since the volume $\mathrm{vol}(K)$ of the compact convex set K is equal to 2^n, we get from Lemma A.2.5 that $\tau_1 \ldots \tau_n \leq 1$ and, hence, that $\tau_n \leq \delta^{-n+1}$. Therefore we can choose n linearly independent polynomials $P_i(t) = a_{i,n-1}t^{n-1} + \ldots + a_{i,1}t + a_{i,0} \in \mathbb{Z}[t]$, satisfying the inequalities

$$\begin{cases} |P_i(x_0)| \leq \delta^{-n+1} \hat{h}\, Q^{-n+1}, \\ |P_i'(x_0)| \leq \delta^{-n+1}\, Q, \\ |a_{i,j}| \leq \delta^{-n+1}\, Q, \quad 2 \leq j \leq n-1. \end{cases} \tag{3.4.3}$$

Applying well-known estimates from the geometry of numbers (see [19, pp. 219]) we obtain

$$D := \det |(a_{i,j-1})_{i,j=1}^{n}| \leq n!.$$

Moreover, from Lemma A.1.19 it follows that there exists a prime number p, which does not divide D and satisfies

$$n! < p < 2n!. \tag{3.4.4}$$

Our next step is to construct the irreducible monic polynomial of degree n using polynomials P_i. Consider the following system of linear equations in n variables $\theta_1, \ldots, \theta_n$

$$\begin{cases} x_0^n + p \sum\limits_{i=1}^{n} \theta_i P_i(x_0) = p(n+1)\delta^{-n+1} \hat{h}\, Q^{-n+1}, \\ n x_0^{n-1} + p \sum\limits_{i=1}^{n} \theta_i P_i'(x_0) = p\, Q + p \sum\limits_{i=1}^{n} |P_i'(x_0)|, \\ \sum\limits_{i=1}^{n} \theta_i a_{i,j} = 0, \quad 2 \leq j \leq n-1. \end{cases} \tag{3.4.5}$$

In order to calculate the determinant $\hat{D}$ of this system, it is convenient to transform it as follows. Multiply the k-th equation, where $k = 3, \ldots, n$, by $p\, x_0^{k-1}$ and subtract it from the first equation of the system (3.4.5). Similarly, multiply the k-th equation, where $k = 3, \ldots, n$, by $p\,(k-1)x_0^{k-2}$ and subtract it from the second equation. After making these transformations the determinant $\hat{D}$ may be written as follows

$$\hat{D} = p^2 \begin{vmatrix} a_{1,1}x_0 + a_{1,0} & \ldots & a_{n,1}x_0 + a_{n,0} \\ a_{1,1} & \ldots & a_{n,1} \\ \vdots & \ddots & \vdots \\ a_{1,n-1} & \ldots & a_{n,n-1} \end{vmatrix}$$

Since the polynomials P_i are linearly independent, we conclude that $\hat{D} = p^2 D \neq 0$. Hence, there exists a unique solution $(\theta_1, \ldots, \theta_n)$ of the system (3.4.5).

For integers $k_1, \ldots, k_n$ consider the following construction, which is a polynomial of degree n with integer coefficients

$$P(t) = t^n + p \sum_{i=1}^{n} k_i P_i(t) = t^n + p\,(a_{n-1}t^{n-1} + \ldots + a_1 t + a_0),$$

where $a_j = \sum\limits_{i=1}^{n} k_i a_{i,j}$ and k_i satisfies

$$|\theta_i - k_i| \leq 1. \tag{3.4.6}$$

The polynomial P is irreducible if it satisfies the conditions of Lemma A.1.20. Let us show that there exists a suitable combinations of the coefficients k_j. Clearly, the first and the second condition of (A.1.6) hold for any k_j. It remains to show that $a_0 = k_1 a_{1,0} + \ldots + k_n a_{n,0}$ is not divisible by p. Since p does not divide D, there exists a number $1 \leq j \leq n$ such that $a_{j,0}$ is not divisible by p. There are two possible values for k_j satisfying the condition (3.4.6), which we denote as k_j^1 and $k_j^2 := k_j^1 + 1$. Then, either $a_0^1 = k_1 a_{1,0} + \ldots + k_j^1 a_{j,0} + \ldots + k_n a_{n,0}$ or $a_0^2 = k_1 a_{1,0} + \ldots + k_j^2 a_{j,0} + \ldots + k_n a_{n,0} = a_0^1 + a_{j,0}$ is not divisible by p. Therefore, choosing k_j in this manner yields an irreducible polynomial P.

Next we estimate the values $|P(x_0)|$, $|P'(x_0)|$ and $H(P)$. Combining (3.4.3) and (3.4.6) with the system of equations (3.4.5) we obtain the following inequalities.

From the first equation of the system it follows that

$$p\delta^{-n+1}\hat{h}\,Q^{-n+1} \leq |P(x_0)| \leq p(2n+1)\delta^{-n+1}\hat{h}\,Q^{-n+1}. \tag{3.4.7}$$

Similarly, from the second equation of the system we have

$$p\,Q \leq |P'(x_0)| \leq (p + 2pn\delta^{-n+1})\,Q, \tag{3.4.8}$$

and the remaining equations of the system give

$$|a_j| \leq n\delta^{-n+1}\,Q, \quad 2 \leq j \leq n-1. \tag{3.4.9}$$

Finally, using (3.4.7)—(3.4.9) and the inequality $|x_0| \leq \frac{3}{2}|d|$ for $Q > Q_0$ we obtain the following estimates for the coefficients a_1 and a_0

$$\begin{aligned} |a_1| &\leq |P'(x_0)| + n|x_0|^{n-1} + \sum_{j=2}^{n-1} j|x_0|^{j-1}|a_j| \\ &\leq (p + 2pn\delta^{-n+1})\,Q + \left(n\delta^{-n+1}\sum_{k=1}^{n-1}(k+1)\left(\tfrac{3}{2}|d|\right)^k\right) Q \\ &\leq \left(p + \left(2p + n\omega_n\left(\tfrac{3}{2}d\right)\right)n\delta^{-n+1}\right)\,Q, \end{aligned} \tag{3.4.10}$$

$$
\begin{aligned}
|a_0| &\le |P(x_0)| + |x_0|^n + |a_1 x_0| + \sum_{j=2}^{n} |x_0|^j |a_j| \\
&\le p(2n+1)\delta^{-n+1}\hat{h}\, Q^{-n+1} + \left(\tfrac{3}{2}p + \left(3p + \tfrac{3}{2}\omega_n\left(\tfrac{3}{2}d\right)\right) n\delta^{-n+1}\right)|d|\, Q \\
&+ \omega_n\left(\tfrac{3}{2}d\right) n\delta^{-n+1}\, Q \le p c_{32}(n,d)\, Q. \qquad (3.4.11)
\end{aligned}
$$

Now, from the estimates (3.4.9)—(3.4.11) and the inequality (3.4.4) we have

$$H(P) \le 2n! c_{33}\, Q =: Q_1. \qquad (3.4.12)$$

Consider the roots $\alpha_1, \dots, \alpha_n$ of the polynomial P, where $|x_0 - \alpha_1| = \min\limits_i |x_0 - \alpha_i|$. Using Lemma A.1.14, we get

$$|x_0 - \alpha_1| \le n|P(x_0)||P'(x_0)|^{-1}. \qquad (3.4.13)$$

Substituting inequalities (3.4.7) and (3.4.8) into (3.4.13) we obtain

$$|x_0 - \alpha_1| \le n(2n+1)\delta^{-n+1}\, Q^{-n} =: c_{34}\, Q^{-n}. \qquad (3.4.14)$$

If α_1 is a complex root of the polynomial P, then its complex conjugate is also a root of the polynomial P. Hence, by (3.4.12), (3.4.14) and the estimates $|\alpha_i| \le H(P)+1$, $1 \le i \le n$ (see [54, Theorem 1.1.2]), we deduce that

$$|P(x_0)| = \prod_{i=1}^{n} |x_0 - \alpha_i| \le c_{34}^2 Q^{-2n} \left(2 + 2n!\left(2n\delta^{-n+1} + 1\right) Q\right)^{n-2}.$$

This inequality contradicts (3.4.7) for $Q > Q_0$. Thus, α_1 is real.

Finally, take a maximal system of real algebraic integers $\Gamma = \{\gamma_1, \dots, \gamma_m\}$ such that $|\gamma_i - \gamma_j| > c_{32}\, Q^{-n}$, $1 \le i \ne j \le m$. Let us show that for any point $x_0 \in B^1$ there exists an algebraic number $\gamma \in \Gamma$ such that $|x_0 - \gamma| \le 2c_{34}\, Q^{-n}$. According to the above arguments and (3.4.14) for any point $x_0 \in B^1$ there exists a real algebraic integer $\alpha_1 \in I$ such that $|x_0 - \alpha_1| \le c_{34}\, Q^{-n}$. If $\alpha_1 \in \Gamma$, then we can take $\gamma = \alpha_1$, otherwise, there exists $\gamma_i \in \Gamma$ such that $|\alpha_1 - \gamma_i| \le c_{34} Q^{-n}$ and, hence,

$$|x_0 - \gamma_i| \le |x_0 - \alpha_1| + |\alpha_1 - \gamma_i| \le 2c_{34} Q^{-n}.$$

In this case, we take $\gamma = \gamma_i$. Therefore,

$$B^1 \subset \bigcup_{i=1}^{m} \left\{x \in I : |x - \gamma_i| \le 2c_{34}\, Q^{-n}\right\}$$

and

$$4mc_{34}\, Q^{-n} \ge \lambda_1\left(\bigcup_{i=1}^{m} \left\{x \in I : |x - \gamma_i| \le 2c_{34}\, Q^{-n}\right\}\right) \ge \lambda_1\left(B^1\right) \ge \tfrac{3}{4}\lambda_1(I).$$

This inequality implies that

$$\mathcal{N}_n(\mathcal{O}, Q_1, I) \ge m > \tfrac{3}{16} c_{34}^{-1} Q^n \lambda_1(I) = c_{26}\, Q_1^n \lambda_1(I)$$

for $Q_1 > Q_0$ and the proof is complete.

From the proof of Theorem 3.4.1 it follows, that the set of algebraic integers of degree n forms a regular system with respect to the function $N(\alpha) = \left(\frac{H(\alpha)}{(1+|\alpha|)^{n-1}}\right)^n$ and $T_0 = c_{35}\lambda_1(I)^{-n}$, where the constant c_{35} is independent of $\lambda_1(I)$.

3.4.1.2 Upper Bound

The proof of upper bound is very similar to the proof of Theorem 3.2.3.

Assume that

$$\mathcal{N}_n(\mathcal{O}, Q, I) > c_{27}\, Q^n \lambda_1(I).$$

Consider a point $\alpha \in \mathbb{A}_n(Q) \cap I$ and let P be its minimal polynomial. Let us derive an estimate for the polynomial P at point d. By Lemma 3.2.4 we have

$$|P^{(k)}(\alpha)| \le \tfrac{n!}{(n-k)!}\, \omega_{n-k+1}(3/2\, d)\, Q,$$

for all $1 \le k \le n$ and $Q > Q_0$. From these estimates and a Taylor expansion of P in the intervals I we obtain

$$|P(d)| \le \sum_{k=1}^{n} \left|\tfrac{1}{k!} P^{(k)}(\alpha)(d-\alpha)^k\right| \le 2^n \omega_n(3/2\, d)\, Q \lambda_1(I). \tag{3.4.15}$$

Let us fix a vector $\mathbf{a} := (a_{n-1}, \dots, a_1) \in \mathbb{Z}^{n-1}$ and denote by $\mathcal{P}_n(Q, \mathbf{a}) \subset \mathcal{P}_n(Q)$ the subclass of polynomials

$$\mathcal{P}_n(Q, \mathbf{a}) := \left\{P \in \mathcal{P}_n(Q) \colon P(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0,\ P \text{ satisfies } (3.4.15)\right\}$$

with the same vector of coefficients $\mathbf{a}$ such that P satisfies (3.4.15). The number of non-empty subclasses $\mathcal{P}_n(Q, \mathbf{a})$ is bounded above by the number of vectors $\mathbf{a} \in [-Q; Q]^{n-1}$, which can be estimated as follows

$$\#\left([-Q; Q]^{n-1} \cap \mathbb{Z}^{n-1}\right) = (2Q+1)^{n-1} < 2^n\, Q^{n-1} \tag{3.4.16}$$

for $Q > Q_0$. This allows us to write

$$c_{27}\, Q^n \lambda_1(I) < \mathcal{N}_n(\mathcal{O}, Q, I) \le n \sum_{\mathbf{a}} \#\mathcal{P}_n(Q, \mathbf{a}).$$

Thus, by the estimate (3.4.16) and pigeonhole principle we conclude that there exists a vector $\mathbf{a}_0$ such that

$$\#\mathcal{P}_n(Q, \mathbf{a}_0) \ge c_{27}\, 2^{-n} n^{-1} Q\, \lambda_1(I). \tag{3.4.17}$$

Let us find an upper bound for the value $\#\mathcal{P}_n(Q, \mathbf{a}_0)$. Fix some polynomial $P_0 \in \mathcal{P}_n(Q, \mathbf{a}_0)$ and consider the difference between the polynomials P_0 and $P_j \in \mathcal{P}_n(Q, \mathbf{a}_0)$ at point d. From the estimate (3.4.15) it follows

$$|P_0(d) - P_j(d)| = |a_{0,0} - a_{j,0}| \le 2^{n+1} \omega_n(3/2\, d)\, Q \lambda_1(I),$$

which contradicts to inequality (3.4.17) for $c_{27} = 2^{2n+4} n \omega_n(3/2\, d)$. Thus the proof is complete.

3.4.2 Proof of Theorem 3.4.3

The proof of Theorem 3.4.3 follows by the same method as the proof of Theorem 3.4.1, but it contains some non-trivial elements which require special attention.

We will start with using Lemma 3.2.6, which is two-dimensional analogue of Lemma 3.4.6. Given positive v_1 and v_2 satisfying the condition $v_1 + v_2 = n - 2$ denote by $L^2 = L_{n-1}(Q, \delta, \mathbf{v}, \Pi)$ the set of points $\mathbf{x} \in \Pi$ such that there exists a polynomials $P \in \mathcal{P}_{n-1}(Q)$ satisfying the inequalities

$$\begin{cases} |P(x_i)| < h\, Q^{-v_i}, \\ \min\limits_i \{|P'(x_i)|\} < \delta\, Q, \quad i = 1, 2. \end{cases} \tag{3.4.18}$$

Lemma 3.2.6 implies that

$$\lambda_2\left(L^2\right) \le \tfrac{1}{4}\,\lambda_2\left(\Pi\right)$$

for $\delta < \delta_0(n-1, \mathbf{d}) < 1$ and $Q > Q_0(n-1, \mathbf{v}, \mathbf{d}, \mathbf{s})$.

Let us consider the set $B^2 := \Pi \backslash L^2$. Using Minkowski's linear form theorem (Lemma A.2.3) it is easy to ckeck that for every point $\mathbf{x} \in \Pi$ there exists a polynomial $P \in \mathcal{P}_{n-1}(Q)$ such that

$$|P(x_i)| \le h\, Q^{-v_i}, \quad i = 1, 2,$$

where $h = \sqrt{\frac{3}{2}}(|d_1| + |d_2|)^{1/2} \max\left(1, 3|d_1|, 3|d_2|\right)^{(n-1)^2/2}$. Hence, for any point $\mathbf{x} \in B^2$ and any polynomial $P \in \mathcal{P}_{n-1}(Q)$ we have

$$\begin{cases} |P(x_i)| < h\, Q^{-v_i}, \\ |P'(x_i)| > \delta\, Q, \quad i = 1, 2. \end{cases}$$

Consider an arbitrary point $\mathbf{x} \in B^2$ and examine the successive minima $\tau_1, \ldots, \tau_n$ of the compact convex set K defined by

$$\begin{cases} \left|a_{n-1}x_i^{n-1} + \ldots + a_1 x_i + a_0\right| \le h\, Q^{-v_i}, \\ \left|(n-1)a_{n-1}x_i^{n-2} + \ldots + 2a_2 x_i + a_1\right| \le Q, \quad i = 1, 2, \\ |a_{n-1}|, \ldots, |a_2| \le Q. \end{cases}$$

Assuming $\tau_1 \le \delta$ we obtain that for sufficiently small δ there exists a polynomial $P \in \mathcal{P}_{n-1}(Q)$ satisfying the inequalities

$$\begin{cases} |P(x_i)| < \delta h\, Q^{-v_i} < h\, Q^{-v_i}, \\ |P'(x_i)| < \delta\, Q, \quad i = 1, 2, \\ H(P) < Q. \end{cases}$$

This leads to a contradiction, since $\mathbf{x} \notin L^2$. Thus, $\tau_1 > \delta$. Since the volume of the compact convex set K is at least 2^n, we conclude by Lemma A.2.3 that $\tau_1 \ldots \tau_n \le 1$

and $\tau_n \le \delta^{-n+1}$. Thus, by definition of successive minima, we can choose n linearly independent polynomials $P_j(t) = a_{j,n-1}t^{n-1} + \ldots + a_{j,1}t + a_{j,0} \in \mathbb{Z}[t]$ satisfying the inequalities

$$\begin{cases} |P_j(x_i)| \le \delta^{-n+1} h\, Q^{-v_i}, \\ |P_j'(x_i)| \le \delta^{-n+1}\, Q, \quad i = 1, 2, \\ |a_{j,k}| \le \delta^{-n+1}\, Q, \quad 4 \le k \le n-1. \end{cases} \tag{3.4.19}$$

with

$$D := \det |(a_{j,k-1})_{j,k=1}^{n}| \le n!.$$

Using Lemma A.1.19 choose a prime p satisfying

$$n! < p < 2n! \tag{3.4.20}$$

and consider a system of linear equations in n variables $\theta_1, \ldots, \theta_n$

$$\begin{cases} x_i^n + p \sum\limits_{j=1}^{n} \theta_j P_j(x_i) = p(n+1)\delta^{-n+1} h\, Q^{-v_i}, \\ n x_i^{n-1} + p \sum\limits_{j=1}^{n} \theta_j P_j'(x_i) = pQ + p \sum\limits_{j=1}^{n} |P_j'(x_i)|, \quad i = 1, 2, \\ \sum\limits_{j=1}^{n} \theta_j a_{j,k-1} = 0, \quad 5 \le k \le n. \end{cases} \tag{3.4.21}$$

Our next goal is to show that the determinant $\hat{D}(\mathbf{x})$ of this system does not vanish. Let us transform the system (3.4.21) as follows. Multiply the k-th equation, where $k = 5, 6, \ldots, n$, by $p\, x_1^{k-1}$ (respectively by $p\, x_2^{k-1}$) and subtract it from the first (respectively the second) equation of the system (3.4.21). Similarly, multiply the k-th equation, where $k = 5, 6, \ldots, n$, by $p\,(k-1)x_1^{k-2}$ (respectively by $p\,(k-1)x_2^{k-2}$) and subtract it from the third (respectively the fourth) equation. After these transformations the determinant of system (3.4.21) may be written as

$$\hat{D}(\mathbf{x}) = p^4 \cdot \begin{vmatrix} \sum\limits_{k=0}^{3} a_{1,k}x_1^k & \ldots & \sum\limits_{k=0}^{3} a_{n,k}x_1^k \\ \sum\limits_{k=0}^{3} a_{1,k}x_2^k & \ldots & \sum\limits_{k=0}^{3} a_{n,k}x_2^k \\ \sum\limits_{k=1}^{3} k \cdot a_{1,k}x_1^{k-1} & \ldots & \sum\limits_{k=1}^{3} k \cdot a_{n,k}x_1^{k-1} \\ \sum\limits_{k=1}^{3} k \cdot a_{1,k}x_2^{k-1} & \ldots & \sum\limits_{k=1}^{3} k \cdot a_{n,k}x_2^{k-1} \\ a_{1,4} & \ldots & a_{n,4} \\ \vdots & \ddots & \vdots \\ a_{1,n-1} & \ldots & a_{n,n-1} \end{vmatrix}.$$

We proceed to show that $\hat{D}(\mathbf{x})$ is equal to D up to a multiple depending only on x_1, x_2 and p. Multiply the third (respectively the fourth) row by $\frac{1}{3}x_1$ (respectively by $\frac{1}{3}x_2$) and subtract it from the first (respectively the second) row. Then subtracting

the first (respectively the third) row from the second (respectively the fourth) row gives:

$$\hat{D}(\mathbf{x}) = \tfrac{p^4(x_2-x_1)^2}{9} \cdot \begin{vmatrix} a_{1,2}x_1^2 + 2a_{1,1}x_1 + 3a_{1,0} & \dots & a_{n,2}x_1^2 + 2a_{n,1}x_1 + 3a_{n,0} \\ a_{1,2}(x_2+x_1) + 2a_{1,1} & \dots & a_{n,2}(x_2+x_1) + 2a_{n,1} \\ 3a_{1,3}x_1^2 + 2a_{1,2}x_1 + a_{1,1} & \dots & 3a_{n,3}x_1^2 + 2a_{n,2}x_1 + a_{n,1} \\ 3a_{1,3}(x_2+x_1) + 2a_{1,2} & \dots & 3a_{n,3}(x_2+x_1) + 2a_{n,2} \\ a_{1,4} & \dots & a_{n,4} \\ \vdots & \ddots & \vdots \\ a_{1,n-1} & \dots & a_{n,n-1} \end{vmatrix}.$$

Now let us subtract the second row multiplied by x_1 from the first row and the fourth row multiplied by $\frac{1}{2}$ from the third row. Then subtract the third row multiplied by $\frac{x_2+x_1}{x_1^2}$ from the fourth row, and finally subtract the fourth row multiplied by x_1x_2, x_2+x_1 and $\frac{3}{2}x_1 - \frac{1}{2}x_2$ from the first, the second and the third row respectively. Consequently we obtain the inequality

$$\hat{D}(\mathbf{x}) = p^4(x_2-x_1)^4 D > 0,$$

since the polynomials P_j are linearly independent and $|x_1 - x_2| > \frac{|d_1-d_2|}{2} > 0$. Hence, the system (3.4.21) has a unique solution $(\theta_1, \dots, \theta_n)$. Moreover, there exist integers $k_1, \dots, k_n$ satisfying

$$|\theta_i - k_i| \le 1, \quad i = 1, \dots, n, \tag{3.4.22}$$

such that the following polynomial with integer coefficients

$$P(t) = t^n + p\sum_{j=1}^{n} k_j P_j(t) = t^n + p\,(a_{n-1}t^{n-1} + \dots + a_1 t + a_0),$$

where $a_k = \sum\limits_{j=1}^{n} k_j a_{j,k}$ is irreducible. This follows by the same arguments as in the previous section.

Let us estimate the values $|P(x_i)|$ and $|P'(x_i)|$. By the inequalities (3.4.19), (3.4.22), and (3.4.21) we obtain

$$p\delta^{-n+1}h\,Q^{-v_i} \le |P(x_i)| \le p(2n+1)\delta^{-n+1}h\,Q^{-v_i}, \quad i = 1, 2, \tag{3.4.23}$$

$$p\,Q \le |P'(x_i)| \le \left(p + 2pn\delta^{-n+1}\right) Q, \quad i = 1, 2. \tag{3.4.24}$$

Finally, we need to estimate the height $H(P)$. By (3.4.21) and inequalities (3.4.19), (3.4.22), we have

$$|a_k| \le n\delta^{-n+1}\,Q, \quad 4 \le k \le n-1. \tag{3.4.25}$$

It remains to estimate $|a_0|$, $|a_1|$, $|a_2|$ and $|a_3|$. By (3.4.23) – (3.4.25) and the inequalities $|x_i| \le |d_i| + \frac{1}{2}$, for $Q > Q_0$ we have

$$|a_3x_i^3 + a_2x_i^2 + a_1x_i + a_0| \le |P(x_i)| + \sum_{k=4}^{n} (|d_i| + 1)^k \, |a_k| < c_{36,i}Q,$$

$$|3a_3x_i^2 + 2a_2x_i + a_1| \le |P'(x_i)| + \sum_{k=4}^{n} k\,(|d_i| + 1)^k \, |a_k| < c_{37,i}Q, \quad i = 1, 2, \quad (3.4.26)$$

where

$$c_{36,i} = \begin{cases} h, & n = 3, \\ 2n\delta^{-n+1}h\,(|d_i| + 1)^n\,, & n > 3; \end{cases} \qquad c_{37,i} = \begin{cases} p + 2pn\delta^{-n+1}h, & n = 3, \\ 4pn^2\delta^{-n+1}h\,(|d_i| + 1)^n\,, & n > 3. \end{cases}$$

We emphasize that in order to simplify equations we do not care about the accuracy of the constants. Consider the following system of linear equations for a_0, a_1, a_2 and a_3

$$\begin{cases} a_3x_i^3 + a_2x_i^2 + a_1x_i + a_0 = l_{1,i}, \\ 3a_3x_i^2 + 2a_2x_i + a_1 = l_{2,i}, \quad i = 1, 2. \end{cases} \quad (3.4.27)$$

According to the above computations the determinant of the system (3.4.27) does not vanish. Thus, the system has a unique solution, which may be found by Cramer's rule. Combining this with estimates (3.4.26), (3.4.20) and $|x_i| \le |d_i| + \frac{1}{2}$ one can easily verify

$$|a_j| < c_{38}\,Q, \quad 0 \le j \le 3.$$

Applying (3.4.25) now yields the following estimate

$$H(P) < \max\left(c_{38}, n\delta^{-n+1}\right) Q =: Q_1. \quad (3.4.28)$$

Consider the roots $\alpha_1, \dots, \alpha_n$ of the polynomial P, where $|x_i - \alpha_i| = \min\limits_j |x_i - \alpha_j|$. By Lemma A.1.14 and estimates (3.4.23), (3.4.24), we have

$$|x_i - \alpha_i| < n(2n + 1)\delta^{-n+1}h\,Q^{-v_i-1} = c_{39}\,Q^{-v_i-1}, \quad i = 1, 2, \quad (3.4.29)$$

where $c_{39} = n(2n + 1)\delta^{-n+1}h$. Let us prove that $\alpha_1, \alpha_2 \in \mathbb{R}$ for $v_1 = v_2 = \frac{n-2}{2}$. Assume the converse: let $\alpha_i \in \mathbb{C}$, then its complex conjugate is also a root of the polynomial P. Hence, by (3.4.28), (3.4.29) and Lemma A.1.18 we conclude that

$$|P(x_i)| = \prod_{j=1}^{n} |x_i - \alpha_j| \le c_{39}^2\,Q^{-n} \cdot c_{40}\,Q = c_{40}c_{39}^2\,Q^{-n+1}.$$

This inequality contradicts (3.4.23) for $Q > Q_0$.

Let $\Gamma = \{\boldsymbol{\gamma}_1, \dots, \boldsymbol{\gamma}_t\}$ be a maximal system of points with real algebraic conjugate integer coordinates satisfying the condition that rectangles

$$\sigma(\boldsymbol{\gamma}_k) := \left\{\mathbf{x} \in \mathbb{R}^2 \colon |x_i - \gamma_{k,i}| < c_{39}\,Q^{-\frac{n}{2}}, i = 1, 2\right\}, \quad 1 \le k \le t,$$

do not intersect. Furthermore, let us introduce the expanded rectangles

$$\sigma'(\boldsymbol{\gamma}_k) := \left\{\mathbf{x} \in \mathbb{R}^2 \colon |x_i - \gamma_{k,i}| < 2c_{39}\, Q^{-\frac{n}{2}}, i = 1, 2\right\}, \qquad 1 \le k \le t,$$

and show that

$$B^2 \subset \bigcup_{k=1}^{t} \sigma'(\boldsymbol{\gamma}_k). \tag{3.4.30}$$

To prove this fact, we are going to show that for any point $\mathbf{x}_1 \in B^2$ there exists a point $\boldsymbol{\gamma}_k \in \Gamma$ such that $\mathbf{x}_1 \in \sigma'(\boldsymbol{\gamma}_k)$. Since $\mathbf{x}_1 \in B^2$, there is an point $\boldsymbol{\alpha}$ with real algebraic conjugate integer coordinates satisfying the inequalities (3.4.29). Thus, either $\boldsymbol{\alpha} \in \Gamma$ and $\mathbf{x}_1 \in \sigma'(\boldsymbol{\alpha})$, or there exists a point $\boldsymbol{\gamma}_k \in \Gamma$ satisfying

$$|\alpha_i - \gamma_{k,i}| \le c_{39}\, Q^{-\frac{n}{2}}, \quad i = 1, 2,$$

which implies that $\mathbf{x}_1 \in \sigma'(\boldsymbol{\gamma}_k)$. Hence, from (3.4.30) and the estimate $\lambda_2\left(B^2\right) \ge \frac{3}{4}\,\lambda_2\left(\Pi\right)$ we have

$$\tfrac{3}{4}\,\lambda_2\left(\Pi\right) \le \lambda_2\left(B^2\right) \le \sum_{k=1}^{t} \lambda_2\left(\sigma_1(\boldsymbol{\gamma}_k)\right) \le t 2^4 c_{39}^2\, Q^{-n},$$

which together with (3.4.28) yields the estimate

$$\mathcal{N}_n^2\left(\mathcal{O}, Q_1, \Pi\right) \ge t \ge c_{28}\, Q_1^n \lambda_2\left(\Pi\right).$$

Chapter 4

Affine Transformation of Random Simplices and Integral Geometry

In this chapter we will consider the random k-dimensional simplices defined as convex hull of random points $X_0, \dots, X_k$ in $\mathbb{R}^n$, $k \leq n$.

Before we start let us recall some definitions. For $k \in \{0, \dots, n\}$, the linear Grassmannian of k-dimensional linear subspaces of $\mathbb{R}^n$ is denoted by $G_{n,k}$ and is equipped with a unique rotation invariant Haar measure $\nu_{n,k}$. Analogously, for $k \in \{0, \dots, n\}$, the affine Grassmannian of k-dimensional affine subspaces of $\mathbb{R}^n$ is denoted by $A_{n,k}$ and is equipped with a unique rigid motion invariant Haar measure $\mu_{n,k}$. It should be noted that $\nu_{n,k}$ is normalized by

$$\nu_{n,k}(G_{n,k}) = 1,$$

which means that $\nu_{n,k}$ is probabilistic measure on $G_{n,k}$. For $L \in G_{n,k}$ or $L \in A_{n,k}$ we denote by λ_L the k-dimensional Lebesgue measures on L. We will denote by $\langle \cdot, \cdot \rangle$ the Euclidean scalar product in $\mathbb{R}^n$ and by $\| \cdot \|_2$ the induced norm.

Some of the sets we consider have dimension less than n. In fact, we consider 3 classes: the convex hulls of $k+1$ points, orthogonal projections to k-dimensional linear subspaces, and intersections with k-dimensional affine subspaces, where $k \in \{0, \dots, n\}$. In this case $\mathrm{vol}(\cdot)$ stands for the k-dimensional volume.

Consider $k+1$ random points $X_0, \dots, X_k$ in $\mathbb{R}^n$ and denote by

$$\mathrm{conv}(X_0, \dots, X_k)$$

their convex hull, which is the the smallest convex set that contains all of them. This convex hull is an example of random polytope with vertices $X_0, \dots, X_k$. If $1 \leq k \leq n$ then the random polytope $\mathrm{conv}(X_0, \dots, X_k)$ is a k-dimensional simplex (maybe degenerate). Denote by

$$\Delta_k(X_0, \dots, X_k) := \mathrm{vol}\left(\mathrm{conv}(X_0, \dots, X_k)\right) \tag{4.0.1}$$

the k-dimensional volume of the simplex $\mathrm{conv}(X_0, \dots, X_k)$. One natural question here is to find the distribution of the random variable $\Delta_k(X_0, \dots, X_k)$. This is very difficult problem. So far it has been studied for a few models of random variables $X_0, \dots, X_k$ only , which were defined in [51] and [56]:

1. The *Gaussian model*: $X_0, \dots, X_k$ are i.i.d. standard Gaussian random vectors with density function

$$f(\|\mathbf{x}\|) = (2\pi)^{-n/2} \exp\left(-\frac{1}{2}\|\mathbf{x}\|^2\right), \quad \mathbf{x} \in \mathbb{R}^n.$$

2. The *Beta model with parameter* $\nu > 0$: $X_0, \dots, X_k$ are i.i.d. points in the unit ball $\mathbb{B}^n$ with density function

$$f(\|\mathbf{x}\|) = \pi^{-n/2} \frac{\Gamma\left(\frac{n+\nu}{2}\right)}{\Gamma\left(\frac{\nu}{2}\right)} \left(1 - \|\mathbf{x}\|^2\right)^{(\nu-2)/2}, \quad \mathbf{x} \in \mathbb{B}^n.$$

3. The *Beta prime model with parameter* $\nu > 0$: $X_0, \dots, X_k$ are i.i.d. points with density function

$$f(\|\mathbf{x}\|) = \pi^{-n/2} \frac{\Gamma\left(\frac{n+\nu}{2}\right)}{\Gamma\left(\frac{\nu}{2}\right)} \left(1 + \|\mathbf{x}\|^2\right)^{-(n+\nu)/2}, \quad \mathbf{x} \in \mathbb{R}^n.$$

4. The *spherical model*: $X_0, \dots, X_k$ are uniformly distributed on the unit sphere centered at the origin of R^n.

The investigation of this problem started with the calculation of the moments

$$\mathbb{E}\left[\Delta_k(X_0, \dots, X_k)^p\right]. \tag{4.0.2}$$

Miles derived exact formulas for (4.0.2) where $X_0, \dots, X_k$ are generated by one of the four models described above: for the Gaussian model and integer $p \geq 0$ see [51, Equation (70)], for the Beta model with parameter $\nu > 0$ and integer $p \geq 0$ see [51, Equation (74)], for the Beta prime model with parameter $\nu > 0$ and integer $0 \leq p < \frac{\nu}{2}$ see [51, Equation (72)]. Those formulas provide a representation of the moments (4.0.2) in terms of Gamma functions. It should be noted that the formula for the spherical model can be easily obtained from the Beta model with parameter $\nu > 0$ by letting $\nu \to 0$. The extension of Miles' result to non-integer moments $p > -1$ has been recently obtained by Kabluchko, Temesvari, and Thäle [42, Proposition 2.8]. The latter result allows to predict the volume distribution of the random simplex $\mathrm{conv}(X_0, \dots, X_k)$ and, finally, using the moments method, Grote, Kobluchko, and Thäle [38, Theorem 2.5] obtained a probabilistic representation of the volume of a random simplex generated by one of the four models.

In next sections we will investigate how the distribution of the volume of random simplex changes under some fixed affine transformation. As an application we derive the new representation of intrinsic volumes of some ellipsoid, obtain integral geometry formula connecting the average volume of projections and the average volume of cross-sections of an ellipsoid, prove the generalization of integral formula of Furstenberg and Tzkoni [30] and establish its affine version.

4.1 Main Result

For a fixed $k \in \{1, \dots, n\}$ consider n-dimensional random vectors $X_0, \dots, X_k$ (not necessarily independent and identically distributed) with an arbitrary *spherically symmetric* joint distribution. By this we mean that the $(k+1)$-tuple $(X_0, \dots, X_k)$ is equidistributed with $(UX_0, \dots, UX_k)$ for any orthogonal $n \times n$ matrix U. Consider some non-degenerate affine transformation on $\mathbb{R}^n$, defined by $\mathbf{x} \to A\mathbf{x}$, where A is non-singular $n \times n$ matrix, and apply this transformation to the simplex $\operatorname{conv}(X_0, \dots, X_k)$.

In those settings one can ask the following question.
Problem 4.1.1. How does the distribution of the volume (4.0.1) changes under the affine transformations?

For $k = n$, the answer is obvious: it is multiplied by the determinant of the transformation, namely for any $\mathbf{x}_0, \dots, \mathbf{x}_n \in \mathbb{R}^n$ we have

$$\Delta_n(A\mathbf{x}_0, \dots, A\mathbf{x}_n) = |\det(A)|\, \Delta_n(\mathbf{x}_0, \dots, \mathbf{x}_n).$$

The case $k < n$ presents a more delicate problem, since the above equality does not hold anymore. The theorem below provides the solution of Problem 4.1.1.
Theorem 4.1.2. *Let A be non-singular $n \times n$ matrix and let $\mathcal{E}$ be the ellipsoid defined by*

$$\mathcal{E} := \left\{ \mathbf{x} \in \mathbb{R}^n : \mathbf{x}^\top (A^\top A)^{-1} \mathbf{x} \le 1 \right\}. \tag{4.1.1}$$

Then we have

$$\Delta_k(AX_0, \dots, AX_k) \stackrel{d}{=} \frac{\operatorname{vol}(P_\xi \mathcal{E})}{\kappa_k} \cdot \Delta_k(X_0, \dots, X_k), \tag{4.1.2}$$

where ξ is random k-dimensional linear subspace, uniformly distributed with respect to $\nu_{n,k}$ and independent of $X_0, \dots, X_k$ and P_L denotes the orthogonal projection operator on k-dimensional linear subspace $L \in G_{n,k}$.

It is obvious that all four density functions described above are spherically symmetric and, thus, (4.1.2) is applicable to those models.

The main ingredients of the proof of Theorem 4.1.2 is the following deterministic version of (4.1.2).
Proposition 4.1.3. *Let A and $\mathcal{E}$ be as in Theorem 4.1.2. Consider the vectors $\mathbf{x}_1, \dots, \mathbf{x}_k \in \mathbb{R}^n$ and denote by L the span (linear hull) of $\mathbf{x}_1, \dots, \mathbf{x}_k$. Then*

$$\Delta_k(0, A\mathbf{x}_1, \dots, A\mathbf{x}_k) = \frac{\operatorname{vol}(P_L \mathcal{E})}{\kappa_k} \cdot \Delta_k(0, \mathbf{x}_1, \dots, \mathbf{x}_k). \tag{4.1.3}$$

Remark 4.1.4. *Let us stress that here the origin is added to the convex hull. This is important for obtaining the deterministic equation.*

4.1.1 Connection with Intrinsic Volumes

The concept of intrinsic volumes is an important characteristic of the convex sets. Given some convex set $K \subset \mathbb{R}^n$, consider its parallel body

$$K_\epsilon := \left\{ \mathbf{x} \in \mathbb{R}^n \colon \inf_{s \in K} \|x - s\|_2 \leq \epsilon \right\}.$$

The volume of K_ϵ is a polynomial in ϵ of degree at most n

$$\mathrm{vol}(K_\epsilon) = \sum_{k=0}^{n} \epsilon^{n-k} \kappa_{n-k} V_k(K).$$

This result is known as the Steiner formula. The functionals $V_0, \ldots, V_n$ are called the intrinsic volumes and they depend only on K and not on the dimension of its surrounding space.

Due to Kubota's formula (C.1.1), the average volume of k-dimensional projection $\mathbb{E}\,\mathrm{vol}(P_\xi \mathcal{E})$ is proportional to the k-th intrinsic volume $V_k(\mathcal{E})$ of the ellipsoid $\mathcal{E}$ (see Section C.1 for more details). Thus, taking expectation in (4.1.2) readily implies the following corollary.

Corollary 4.1.4.1. *Under the assumptions of Theorem 4.1.2 we have*

$$\mathbb{E}\left[\Delta_k(AX_0, \ldots, AX_k)\right] = \binom{n}{k}^{-1} \frac{\kappa_{n-k}}{\kappa_n} V_k(\mathcal{E})\, \mathbb{E}\left[\Delta_k(X_0, \ldots, X_k)\right]. \tag{4.1.4}$$

The formula for $V_k(\mathcal{E})$ was derived in [68]. Relation (4.1.4) can be generalized to higher moments using the notion of *generalized* intrinsic volumes introduced in [21].

4.1.2 Connection with Gaussian Random Matrices

The next point to be mentioned is that the distribution of the volume of a random projection $P_\xi \mathcal{E}$ is not known and even moments would be difficult to find in general. This fact makes the equation (4.1.2) less convenient to use. We can get rid of this problem finding a representation of the random variable $\mathrm{vol}\,(P_\xi \mathcal{E})$ in terms of the determinants of Gaussian random matrices.

Theorem 4.1.5. *Under the assumptions of Theorem 4.1.2 we have*

$$\frac{\mathrm{vol}(P_\xi \mathcal{E})}{\kappa_k} \stackrel{d}{=} \left(\frac{\det\left(G^\top A^\top A G\right)}{\det\left(G^\top G\right)} \right)^{1/2} \stackrel{d}{=} \left(\frac{\det\left(G_{\mathbf{a}}^\top G_{\mathbf{a}}\right)}{\det\left(G^\top G\right)} \right)^{1/2}, \tag{4.1.5}$$

where G is a random $n \times k$ matrix with i.i.d. standard Gaussian entries N_{ij} and $G_{\mathbf{a}}$ is a random $n \times k$ matrix with the entries $a_i N_{ij}$, where $a_1, \ldots, a_n$ denote the singular values of A.

Using the representation (4.1.5), we obtain the following version of (4.1.2).

Corollary 4.1.5.1. *Under the assumptions of Theorem 4.1.2 we have*

$$\Delta_k(AX_0,\dots,AX_k) \stackrel{d}{=} \left(\frac{\det\left(G^\top A^\top AG\right)}{\det\left(G^\top G\right)}\right)^{1/2} \Delta_k(X_0,\dots,X_k)$$
$$\stackrel{d}{=} \left(\frac{\det\left(G_{\mathbf{a}}^\top G_{\mathbf{a}}\right)}{\det\left(G^\top G\right)}\right)^{1/2} \Delta_k(X_0,\dots,X_k),$$

where the random matrices G and $G_{\mathbf{a}}$ are defined as in Theorem 4.1.5.

The important special case $k=1$ corresponds to the distance between two random points.

Corollary 4.1.5.2. *For any non-singular $n\times n$ matrix A with singular values $a_1,\dots,a_n$ we have*

$$\|AX_0-AX_1\|_2 \stackrel{d}{=} \sqrt{\frac{a_1^2N_1^2+\dots+a_n^2N_n^2}{N_1^2+\dots+N_n^2}}\cdot\|X_0-X_1\|_2,$$

where $N_1,\dots,N_n$ are i.i.d. standard Gaussian random variables.

These results will be used in the next subsection to study integral geometry problems for ellipsoids.

4.2 Random Points in Ellipsoids

Suppose that $X_0,\dots,X_k$ are independent, identically distributed random n-dimensional vectors, which are uniformly distributed in some convex set $K\subset\mathbb{R}^n$ with non-empty interior (denote by $\sim U(K)$). A classical problem of stochastic geometry is to find the distribution of $\Delta_k(X_0,\dots,X_k)$ starting with its moments

$$\mathbb{E}\left[\Delta_k(X_0,\dots,X_k)^p\right] = \frac{1}{(\mathrm{vol}(K))^{k+1}}\int\limits_{K^{k+1}}\Delta_k(\mathbf{x}_0,\dots,\mathbf{x}_k)^p\,\mathrm{d}\mathbf{x}_0\dots\mathrm{d}\mathbf{x}_k. \tag{4.2.1}$$

To the best of our knowledge, for general K a formula for (4.2.1) is not known even for $n=2, k=p=1$, where the problem reduces to the calculating the mean distance between two random points uniformly chosen in a planar convex set (see [15], [31], [57, Chapter 4], [50, Chapter 2], [5]).

The case of arbitrary k and n was studied for K being a ball only. In [51] it was shown (see also [59, Theorem 8.2.3]) that for $X_0,\dots,X_k\sim U(\mathbb{B}^n)$ and any integer $p\geq 0$ we have

$$\mathbb{E}\left[\Delta(X_0,\dots,X_k)^p\right] = \frac{\kappa_{n+p}^{k+1}}{\kappa_n^{k+1}}\,\frac{\kappa_{k(n+p)+n}}{\kappa_{(k+1)(n+p)}}\,\frac{b_{n,k}}{b_{n+p,k}}, \tag{4.2.2}$$

where κ_k are defined in (C.0.1) and $b_{q,k}$ are defined in (C.0.2). In [42, Proposition 2.8 and p.23] this relation was extended to all real $p>-1$. Theorem 4.1.2 implies the following generalization of (4.2.2) for the ellipsoids.

Theorem 4.2.1. *For any non-degenerate ellipsoid $\mathcal{E} \subset \mathbb{R}^n$ consider random n-dimensional vectors $X_0, \dots, X_k$ uniformly distributed in ellipsoid $\mathcal{E}$. Then any real number $p > -1$ we have*

$$\mathbb{E}\left[\Delta_k(X_0, \dots, X_k)^p\right] = \frac{1}{(k!)^p} \frac{\kappa_{n+p}^{k+1}}{\kappa_n^{k+1}} \frac{\kappa_{k(n+p)+d}}{\kappa_{(k+1)(n+p)}} \frac{b_{n,k}}{b_{n+p,k}} \frac{\mathbb{E}\left[\operatorname{vol}(P_\xi \mathcal{E})^p\right]}{\kappa_k^p}, \tag{4.2.3}$$

where ξ is a uniformly chosen random k-dimensional linear subspace in $\mathbb{R}^n$, independent of $X_0, \dots, X_k$.

Note that (4.2.3) is indeed a generalization of (4.2.2) since $P_\xi \mathbb{B}^n = \mathbb{B}^k$ almost surely and $\operatorname{vol}(\mathbb{B}^k)^p = \kappa_k^p$. For $k = 1$ formula (4.2.3) was recently obtained in [39].

By Kubota's formula (C.1.1), the right-hand side of (4.2.3) with $p = 1$ is proportional to the k-th intrinsic volume of $\mathcal{E}$, which implies the following result.

Corollary 4.2.1.1. *For any non-degenerate ellipsoid $\mathcal{E} \subset \mathbb{R}^n$ consider random n-dimensional vectors $X_0, \dots, X_k$ uniformly distributed in ellipsoid $\mathcal{E}$. Then,*

$$\mathbb{E}\left[\Delta_k(X_0, \dots, X_k)\right] = \frac{1}{2^k} \frac{((n+1)!)^{k+1}}{((n+1)(k+1))!} \left(\frac{\kappa_{n+1}^{k+1}}{\kappa_{(n+1)(k+1)}}\right)^2 V_k(\mathcal{E}).$$

Very recently, for random n-dimensional vectors $X_0, \dots, X_k$ uniformly distributed in the unit ball $\mathbb{B}^n$, a formula for the distribution of $\Delta_k(X_0, \dots, X_k)$ has been derived [38]. For a random variable η and positive $\alpha_1, \alpha_2 > 0$ we write $\eta \sim B(\alpha_1, \alpha_2)$ to denote that η has a Beta distribution with parameters α_1, α_2 and the density

$$\frac{\Gamma(\alpha_1 + \alpha_2)}{\Gamma(\alpha_1)\,\Gamma(\alpha_2)}\, t^{\alpha_1 - 1} (1-t)^{\alpha_2 - 1}, \quad t \in (0,1).$$

It was shown in [38] that for random n-dimensional vectors $X_0, \dots, X_k$ uniformly distributed in unit ball $\mathbb{B}^n$ the following holds

$$(k!)^2\, \eta (1-\eta)^k\, \Delta_k(X_0, \dots, X_k)^2 \stackrel{d}{=} (1-\eta')^k\, \eta_1 \cdots \eta_k, \tag{4.2.4}$$

where $\eta, \eta', \eta_1, \dots, \eta_k$ are independent random variables independent of $X_0, \dots, X_k$, such that

$$\eta, \eta' \sim B\left(\frac{n}{2} + 1, \frac{kn}{2}\right), \quad \eta_i \sim B\left(\frac{n-k+i}{2}, \frac{k-i}{2} + 1\right).$$

Multiplying both sides of (4.2.4) by $\operatorname{vol}(P_\xi \mathcal{E})^2 / \kappa_k^2$ and applying Theorem 4.1.2 and Theorem 4.1.5 leads to the following generalization of (4.2.4).

Theorem 4.2.2. *For any non-degenerate ellipsoid $\mathcal{E} \subset \mathbb{R}^n$ consider random n-dimensional vectors $X_0, \dots, X_k$ uniformly distributed in the ellipsoid $\mathcal{E}$. Then, we have*

$$\begin{aligned}(k!)^2\, \eta\, (1-\eta)^k\, \Delta_k(X_0, \dots, X_k)^2 &\stackrel{d}{=} \kappa_k^{-2}\, (1-\eta')^k\, \eta_1 \cdots \eta_k\, \operatorname{vol}(P_\xi \mathcal{E})^2 \\ &\stackrel{d}{=} (1-\eta')^k\, \eta_1 \cdots \eta_k \left(\frac{\det\left(G_{\mathbf{a}}^\top G_{\mathbf{a}}\right)}{\det\left(G^\top G\right)}\right),\end{aligned}$$

where G is a random $n \times k$ matrix with i.i.d. standard Gaussian entries N_{ij}, $G_{\mathbf{a}}$ is a random $n \times k$ matrix with the entries $a_i N_{ij}$ and $a_1, \dots, a_n$ are the length of semi-axes of $\mathcal{E}$.

Taking $k = 1$ yields the following stochastic equality for the distribution of the distance between two random points in ellipsoid $\mathcal{E}$.

Corollary 4.2.2.1. *Under the assumptions of Theorem 4.2.2 we have*

$$\eta(1-\eta) \cdot \|X_0 - X_1\|_2^2 \stackrel{d}{=} (1-\eta')\,\eta_1 \left(\frac{a_1^2 N_1^2 + \dots + a_n^2 N_n^2}{N_1^2 + \dots + N_n^2} \right),$$

where $N_1, \dots, N_n$ are i.i.d. standard Gaussian random variables.

4.3 Integral Geometry Formulas

For an arbitrary convex compact body K, any real $p > -n$, and $k = 1$ it is possible to express (4.2.1) in terms of the lengths of the one-dimensional sections of K [20, 43]:

$$\int\limits_{K^2} \|\mathbf{x}_0 - \mathbf{x}_1\|_2^p \, \mathrm{d}\mathbf{x}_0 \mathrm{d}\mathbf{x}_1 = \frac{2n\kappa_n}{(n+p)\,(n+p+1)} \int\limits_{A_{n,1}} \mathrm{vol}\,(K \cap E)^{p+n+1}\, \mu_{n,1}(dE).$$

This formula can not be extended to $k > 1$ for arbitrary convex body K, but for ellipsoids $K = \mathcal{E}$ this is possible.

Theorem 4.3.1. *For any non-degenerate ellipsoid $\mathcal{E} \subset \mathbb{R}^n$, any integer $0 \le k \le n$, and any real $p > -n + k - 1$ we have*

$$\int\limits_{\mathcal{E}^{k+1}} \Delta_k(\mathbf{x}_0, \dots, \mathbf{x}_k)^p \, \mathrm{d}\mathbf{x}_0 \dots \mathrm{d}\mathbf{x}_k$$
$$= \frac{1}{(k!)^p} \frac{\kappa_{n+p}^{k+1}}{\kappa_k^{p+n+1}} \frac{\kappa_{k(n+p)+k}}{\kappa_{(k+1)(n+p)}} \frac{b_{n,k}}{b_{n+p,k}} \int\limits_{A_{n,k}} \mathrm{vol}\,(\mathcal{E} \cap E)^{p+n+1}\, \mu_{n,k}(dE). \quad (4.3.1)$$

Combining this theorem with Theorem 4.2.1 readily gives the following connection between the average volumes of k-dimensional cross-sections and projections of an ellipsoid.

Theorem 4.3.2. *For any non-degenerate ellipsoid $\mathcal{E} \subset \mathbb{R}^n$, any integer $0 \le k \le n$, and any real $p \ge 0$ we have*

$$\frac{\kappa_n^{k+1}}{\kappa_k^{n+1}} \frac{\kappa_{k(n+p)+k}}{\kappa_{k(n+p)+n}} \int\limits_{A_{n,k}} \mathrm{vol}\,(\mathcal{E} \cap E)^{p+n+1}\, \mu_{n,k}(dE)$$
$$= \mathrm{vol}(\mathcal{E})^{k+1} \int\limits_{G_{n,k}} \mathrm{vol}\,(P_L \mathcal{E})^p \, \nu_{n,k}(dL).$$

For $p = 0$, we obtain the following integral formula.

Corollary 4.3.2.1. *For any non-degenerate ellipsoid $\mathcal{E} \subset \mathbb{R}^n$ and any integer $0 \leq k \leq n$ we have*

$$\int\limits_{A_{n,k}} \operatorname{vol}(\mathcal{E} \cap E)^{n+1} \, \mu_{n,k}(dE) = \frac{\kappa_k^{n+1}}{\kappa_n^{k+1}} \frac{\kappa_{n(k+1)}}{\kappa_{k(n+1)}} \operatorname{vol}(\mathcal{E})^{k+1}. \tag{4.3.2}$$

This result may be regarded as an affine version of the following integral formula of Furstenberg and Tzkoni [30]:

$$\int\limits_{G_{n,k}} \operatorname{vol}(\mathcal{E} \cap L)^n \, \nu_{n,k}(dL) = \frac{\kappa_k^n}{\kappa_n^k} \operatorname{vol}(\mathcal{E})^k.$$

Our next theorem generalizes this formula in the same way as (4.3.1) generalizes (4.3.2).

Theorem 4.3.3. *For any non-degenerate ellipsoid $\mathcal{E} \subset \mathbb{R}^n$, any integer $0 \leq k \leq n$, and any real $p > -n + k$ we have*

$$\int\limits_{\mathcal{E}^k} \Delta_k(0, \mathbf{x}_1, \ldots, \mathbf{x}_k)^p \, \mathrm{d}\mathbf{x}_1 \ldots \mathrm{d}\mathbf{x}_k = \frac{1}{(k!)^p} \frac{\kappa_{n+p}^k}{\kappa_k^{p+n}} \frac{b_{n,k}}{b_{n+p,k}} \int\limits_{G_{n,k}} \operatorname{vol}(\mathcal{E} \cap L)^{p+n} \, \nu_{n,k}(dL). \tag{4.3.3}$$

In probabilistic language it may be formulated as

$$\mathbb{E}\left[\Delta_k(0, X_1, \ldots, X_k)^p\right] = \frac{1}{(k!)^p} \frac{\kappa_{n+p}^k}{\kappa_k^{p+n}} \frac{b_{n,k}}{b_{n+p,k}} \mathbb{E}\left[\operatorname{vol}(\mathcal{E} \cap \xi)^{p+n}\right],$$

where $X_1, \ldots, X_k$ are independent, identically distributed random vectors uniformly distributed in $\mathcal{E}$ and ξ is a uniformly chosen random k-dimensional linear subspace in $\mathbb{R}^n$.

4.4 Proofs: Part I

4.4.1 Proof of Proposition 4.1.3

To avoid trivialities we assume that $\dim L = k$, i.e. $\mathbf{x}_1, \ldots, \mathbf{x}_k$ are in general position. Let $\mathbf{e}_1, \ldots, \mathbf{e}_k \in \mathbb{R}^n$ be some orthonormal basis in L. Let O_L and X denote $n \times k$ matrices whose columns are $\mathbf{e}_1, \ldots, \mathbf{e}_k$ and $\mathbf{x}_1, \ldots, \mathbf{x}_k$ respectively. It is easy to check that $O_L O_L^\top$ is a $n \times n$ matrix corresponding to the orthogonal projection operator P_L. Thus,

$$O_L O_L^\top X = X. \tag{4.4.1}$$

Recall that $\mathcal{E}$ is defined by (4.1.1). It is known (see, e.g., [60, Appendix H]) that the orthogonal projection $P_L\mathcal{E}$ is an ellipsoid in L and

$$\operatorname{vol}(P_L\mathcal{E}) = \kappa_k \Big[\det\Big(O_L^\top H O_L\Big) \Big]^{1/2}, \tag{4.4.2}$$

where

$$H := A^\top A.$$

A well-known formula for the volume of a k-dimensional parallelepiped and (C.2.1) implies that for any $\mathbf{x}_1, \dots, \mathbf{x}_k \in \mathbb{R}^n$, we have

$$\Delta_k(0, \mathbf{x}_1, \dots, \mathbf{x}_k) = \frac{1}{k!} \Big[\det\Big(X^\top X\Big) \Big]^{1/2}. \tag{4.4.3}$$

Therefore,

$$k!\, \Delta_k(0, A\mathbf{x}_1, \dots, A\mathbf{x}_k) = \Big[\det\Big((AX)^\top AX\Big) \Big]^{1/2} = \Big[\det\Big(X^\top H X\Big) \Big]^{1/2}.$$

Applying (4.4.1) produces

$$\begin{aligned}
\det\Big(X^\top H X\Big) &= \det\Big(X^\top O_L O_L^\top H O_L O_L^\top X\Big) \\
&= \det\Big(O_L^\top H O_L\Big) \det\Big(X^\top O_L\Big) \det\Big(O_L^\top X\Big) \\
&= \det\Big(O_L^\top H O_L\Big) \det\Big(X^\top O_L O_L^\top X\Big) \\
&= \det\Big(O_L^\top H O_L\Big) \det\Big(X^\top X\Big),
\end{aligned}$$

which together with (4.4.2) and (4.4.3) finishes the proof.

4.4.2 Proof of Theorem 4.1.2

We will introduce two proofs of the Theorem 4.1.2. The first proof is simple and straight forward. It does not require the existence of joint density of $X_0, \dots, X_k$. The second proof is based on the Blaschke-Petkantschin formula and the characteristic function uniqueness theorem. The similar approach will be used to prove Theorems 4.3.1 and 4.3.3. In the second proof we will assume that the joint density function of $X_0, \dots, X_k$ exists.

The first proof

Fist of all note that with probability one the equation

$$\frac{\operatorname{vol}(P_\xi \mathcal{E})}{\kappa_k} \cdot \Delta_k(X_0, \dots, X_k) = 0$$

holds if and only if

$$\Delta_k(AX_0, \dots, AX_k) = 0,$$

which in turn is equivalent to

$$\dim \operatorname{conv}(X_0, \dots, X_k) < k.$$

Therefore to prove (4.1.2) it is enough to show that the conditional distributions of $\Delta_k(AX_0, \dots, AX_k)$ and $\frac{\operatorname{vol}(P_\xi \mathcal{E})}{\kappa_k} \cdot \Delta_k(X_0, \dots, X_k)$ given $\dim \operatorname{conv}(X_0, \dots, X_k) = k$ are equal. Thus without loss of generality we can assume that the simplex $\operatorname{conv}(X_0, \dots, X_k)$ is not degenerate with probability one.

Since the joint distribution of $X_0, \dots, X_k$ is spherically symmetric, for any orthogonal matrix U we have

$$\begin{aligned} \Delta_k(AX_0, \dots, AX_k) &= \Delta_k(0, A(X_1 - X_0), \dots, A(X_k - X_0) \\ &\stackrel{d}{=} \Delta_k(0, A(UX_1 - UX_0), \dots, A(UX_k - UX_0). \end{aligned} \tag{4.4.4}$$

Now let Υ be a random orthogonal matrix chosen uniformly from $SO(n)$ with respect to the probabilistic Haar measure and independently of $X_0, \dots, X_k$. The linear span of $X_1 - X_0, \dots, X_k - X_0$ is a k-dimensional linear subspace of $\mathbb{R}^n$. Thus,

$$\xi := \operatorname{span}(0, \Upsilon X_1 - \Upsilon X_0, \dots, \Upsilon X_k - \Upsilon X_0)$$

is a random uniformly chosen k-dimensional linear subspace independent of $X_0, \dots, X_k$. Applying Proposition 4.1.3 to the vectors $\Upsilon X_1 - \Upsilon X_0, \dots, \Upsilon X_k - \Upsilon X_0$ we obtain

$$\begin{aligned} &\Delta_k(0, A(\Upsilon X_1 - \Upsilon X_0), \dots, A(\Upsilon X_k - \Upsilon X_0) \\ &\qquad = \frac{\operatorname{vol}(P_\xi \mathcal{E})}{\kappa_k} \cdot \Delta_k(0, \Upsilon X_1 - \Upsilon X_0, \dots, \Upsilon X_k - \Upsilon X_0) \\ &\qquad = \frac{\operatorname{vol}(P_\xi \mathcal{E})}{\kappa_k} \cdot \Delta_k(\Upsilon X_0, \Upsilon X_1, \dots, \Upsilon X_k) \\ &\qquad \stackrel{d}{=} \frac{\operatorname{vol}(P_\xi \mathcal{E})}{\kappa_k} \cdot \Delta_k(X_0, X_1, \dots, X_k). \end{aligned}$$

Combining this with (4.4.4) for $U = \Upsilon$ finishes the proof.

The second proof

Denote by $f(\mathbf{x}_0, \dots, \mathbf{x}_k)$ the joint density function of $(X_0, \dots, X_k)$. Let

$$\begin{aligned} \varphi_A(t) :&= \int\limits_{(\mathbb{R}^n)^{k+1}} \exp\left(it \log \Delta_k(A\mathbf{x}_0, \dots, A\mathbf{x}_k)\right) f(\mathbf{x}_0, \dots, \mathbf{x}_k)\, \mathrm{d}\mathbf{x}_0 \dots \mathrm{d}\mathbf{x}_k \\ &= \int\limits_{(\mathbb{R}^n)^{k+1}} \exp\left(it \log \Delta_k(0, A(\mathbf{x}_1 - \mathbf{x}_0), \dots, A(\mathbf{x}_k - \mathbf{x}_0))\right) \\ &\quad \times f(\mathbf{x}_0, \dots, \mathbf{x}_k)\, \mathrm{d}\mathbf{x}_0 \dots \mathrm{d}\mathbf{x}_k \end{aligned}$$

be a characteristic function of $\log \Delta_k(AX_0, \dots, AX_k)$. In particular, denoting by I the identity matrix, we obtain that $\varphi_I(t)$ is a characteristic function of $\log \Delta_k(X_0, \dots, X_k)$. Substituting $\mathbf{y}_0 = \mathbf{x}_0$ and $\mathbf{y}_i = \mathbf{x}_i - \mathbf{x}_0$ for $1 \le i \le k$ leads to

$$\begin{aligned}\varphi_A(t) = &\int\limits_{(\mathbb{R}^n)^{k+1}} \exp\left(it \log |\operatorname{conv}(0, A\mathbf{y}_1, \dots, A\mathbf{y}_k)|\right) \\ &\times f(\mathbf{y}_0, \mathbf{y}_1 + \mathbf{y}_0 \dots, \mathbf{y}_k + \mathbf{y}_0)\, \mathrm{d}\mathbf{y}_0 \dots \mathrm{d}\mathbf{y}_k \\ = &\int\limits_{(\mathbb{R}^n)^{k}} \exp\left(it \log |\operatorname{conv}(0, A\mathbf{y}_1, \dots, A\mathbf{y}_k)|\right) g(\mathbf{y}_1, \dots, \mathbf{y}_k)\, \mathrm{d}\mathbf{y}_1 \dots \mathrm{d}\mathbf{y}_k,\end{aligned}$$

where

$$g(\mathbf{y}_1, \dots, \mathbf{y}_k) := \int\limits_{\mathbb{R}^n} f(\mathbf{y}_0, \mathbf{y}_1 + \mathbf{y}_0 \dots, \mathbf{y}_k + \mathbf{y}_0)\, \mathrm{d}\mathbf{y}_0.$$

Using the linear Blaschke-Petkantschin formula (see (C.2.2)) with

$$h(\mathbf{y}_1, \dots, \mathbf{y}_k) := \exp\left(it \log \Delta_k(0, A\mathbf{y}_1, \dots, A\mathbf{y}_k)\right) g(\mathbf{y}_1, \dots, \mathbf{y}_k)$$

gives

$$\begin{aligned}\varphi_A(t) = b_{n,k}(k!)^{n-k} &\int\limits_{G_{n,k}} \int\limits_{L^k} \exp\left(it \log \Delta_k(0, A\mathbf{y}_1, \dots, A\mathbf{y}_k)\right) g(\mathbf{y}_1, \dots, \mathbf{y}_k) \\ &\times \Delta_k(0, \mathbf{y}_1, \dots, \mathbf{y}_k)^{n-k}\, \lambda_L(d\mathbf{y}_1) \dots \lambda_L(d\mathbf{y}_k)\, \nu_{n,k}(dL). \qquad (4.4.5)\end{aligned}$$

Applying Proposition 4.1.3 to (4.4.5) leads to

$$\begin{aligned}\varphi_A(t) = b_{n,k}(k!)^{n-k} &\int\limits_{G_{n,k}} \exp\left(it \log \frac{\operatorname{vol}(P_L \mathcal{E})}{\kappa_k}\right) \int\limits_{L^k} \exp\left(it \log \Delta_k(0, \mathbf{y}_1, \dots, \mathbf{y}_k)\right) \\ &\times g(\mathbf{y}_1, \dots, \mathbf{y}_k) \Delta_k(0, \mathbf{y}_1, \dots, \mathbf{y}_k)^{n-k}\, \lambda_L(d\mathbf{y}_1) \dots \lambda_L(d\mathbf{y}_k)\, \nu_{n,k}(dL).\end{aligned}$$

Since f is spherically symmetric, the function

$$\begin{aligned}h_A(t) := b_{n,k}(k!)^{n-k} &\int\limits_{L^k} \exp\left(it \log \Delta_k(0, \mathbf{y}_1, \dots, \mathbf{y}_k)\right) g(\mathbf{y}_1, \dots, \mathbf{y}_k) \\ &\times \Delta_k(0, \mathbf{y}_1, \dots, \mathbf{y}_k)^{n-k}\, \lambda_L(d\mathbf{y}_1) \dots \lambda_L(d\mathbf{y}_k)\end{aligned}$$

does not depend on the choice of L. Indeed, consider any $L' \in G_{n,k}$. There exists an orthogonal matrix U such that $L = UL'$. Substituting $y_i = Uz_i$ gives

$$\begin{aligned}h_A(t) = b_{n,k}(k!)^{n-k} &\int\limits_{L'^k} \exp\left(it \log \Delta_k(0, U\mathbf{z}_1, \dots, U\mathbf{z}_k)\right) g(U\mathbf{z}_1, \dots, U\mathbf{z}_k) \\ &\times \Delta_k(0, U\mathbf{z}_1, \dots, U\mathbf{z}_k)^{n-k}\, \lambda'_L(d\mathbf{z}_1) \dots \lambda'_L(d\mathbf{z}_k).\end{aligned}$$

Now the claim follows from

$$\Delta_k(0, U\mathbf{z}_1, \dots, U\mathbf{z}_k) = \Delta_k(0, \mathbf{z}_1, \dots, \mathbf{z}_k)$$

and

$$\begin{aligned} g(U\mathbf{z}_1, \dots, U\mathbf{z}_k) &= \int\limits_{\mathbb{R}^n} f(\mathbf{y}_0, U\mathbf{z}_1 + \mathbf{y}_0 \dots, U\mathbf{z}_k + \mathbf{y}_0)\, \mathrm{d}\mathbf{y}_0 \\ &= \int\limits_{\mathbb{R}^n} f(U\mathbf{y}_0, U\mathbf{z}_1 + U\mathbf{y}_0 \dots, U\mathbf{z}_k + U\mathbf{y}_0)\, \mathrm{d}\mathbf{y}_0 \\ &= \int\limits_{\mathbb{R}^n} f(\mathbf{y}_0, \mathbf{z}_1 + \mathbf{y}_0 \dots, \mathbf{z}_k + \mathbf{y}_0)\, \mathrm{d}\mathbf{y}_0 \\ &= g(\mathbf{z}_1, \dots, \mathbf{z}_k), \end{aligned}$$

where at the second step we did a change of variables $\mathbf{y}_0 \to U\mathbf{y}_0$ and at the third step we used the spherical symmetry of f.

Thus $h_A(t)$ does not depend on the choice of L, which implies

$$\varphi_A(t) = h_A(t)\, \mathbb{E} \exp\left(it \log \frac{\mathrm{vol}\,(P_\xi \mathcal{E})}{\kappa_k} \right).$$

In particular,

$$\varphi_I(t) = h_A(t).$$

Comparing the last two equalities and applying the characteristic function uniqueness theorem, we arrive at

$$\log \Delta_k(AX_0, \dots, AX_k) \stackrel{d}{=} \log \frac{\mathrm{vol}\,(P_\xi \mathcal{E})}{\kappa_k} + \log \Delta_k(X_0, \dots, X_k),$$

and the theorem follows.

4.4.3 Proof of Corollary 4.1.5

Denote by $G_1, \dots, G_k \in \mathbb{R}^d$ the columns of the matrix G. Hence, $AG_1, \dots, AG_k \in \mathbb{R}^d$ are the columns of the matrix AG. Using Proposition 4.1.3 with $\mathbf{x}_i = G_i$ and applying (4.4.3) to G and AG gives

$$\left[\det\left(G^\top A^\top A G \right) \right]^{1/2} = \frac{\mathrm{vol}\,(P_\eta \mathcal{E})}{\kappa_k} \cdot \left[\det\left(G^\top G \right) \right]^{1/2},$$

or

$$\left(\frac{\det\left(G^\top A^\top A G \right)}{\det\left(G^\top G \right)} \right)^{1/2} = \frac{\mathrm{vol}\,(P_\eta \mathcal{E})}{\kappa_k},$$

where η is the linear hull of $G_1, \dots, G_k$. Since $G_1, \dots, G_k$ are i.i.d. standard Gaussian vectors, η is uniformly distributed in $G_{n,k}$ with respect to $\nu_{n,k}$, given $\dim \eta = k$, which holds a.s. This implies $\eta \stackrel{d}{=} \xi$, and the corollary follows.

4.4.4 Proofs of Theorem 4.2.1 and Theorem 4.2.2

For any non-degenerate ellipsoid $\mathcal{E}$ there exist a unique *symmetric* positive-definite $n \times n$ matrix A such that

$$\mathcal{E} = A\mathbb{B}^n = \left\{\mathbf{x} \in \mathbb{R}^n \colon \|A^{-1}\mathbf{x}\| \le 1\right\} = \left\{\mathbf{x} \in \mathbb{R}^n \colon \mathbf{x}^\top A^{-2}\mathbf{x} \le 1\right\}.$$

Since $X_0, \dots, X_k$ are i.i.d. random vectors uniformly distributed in $\mathcal{E}$, we have that $A^{-1}X_0, \dots, A^{-1}X_k$ are i.i.d. random vectors uniformly distributed in $\mathbb{B}^n$. It follows from Theorem 4.1.2 that

$$\begin{aligned} \Delta_k(X_0, \dots, X_k) &= \Delta_k(AA^{-1}X_0, \dots, AA^{-1}X_k) \\ &\overset{d}{=} \Delta_k(A^{-1}X_0, \dots, A^{-1}X_k)\, \frac{\operatorname{vol}(P_\xi \mathcal{E})}{\kappa_k}. \end{aligned} \tag{4.4.6}$$

Taking the p-th moment and applying (4.2.2) implies Theorem 4.2.1.

Now apply (4.2.4) to $A^{-1}X_0, \dots, A^{-1}X_k$ we get

$$(k!)^2\, \eta(1-\eta)^k\, \Delta_k(A^{-1}X_0, \dots, A^{-1}X_k)^2 \overset{d}{=} (1-\eta')^k\, \eta_1 \cdots \eta_k.$$

Multiplying by $\frac{\operatorname{vol}(P_\xi \mathcal{E})}{\kappa_k}$ and applying (4.4.6) implies Theorem 4.2.2.

4.4.5 Proof of Corollary 4.2.1.1

From Kubota's formula (see (C.1.1)) and Theorem 4.2.1 we have

$$\mathbb{E}\left[\Delta_k(X_0, \dots, X_k)\right] = \alpha_{n,k}\, V_k(\mathcal{E}),$$

where

$$\alpha_{n,k} := \frac{1}{k!} \frac{\kappa_{n+1}^{k+1}}{\kappa_n^{k+1}} \frac{\kappa_{k(n+1)+n}}{\kappa_{(k+1)(n+1)}} \frac{b_{n,k}}{b_{n+1,k}} \frac{\kappa_{n-k}}{\binom{n}{k}\, \kappa_n}.$$

From the definition of $b_{n,k}$ (see (C.0.2)) and κ_p (see (C.0.1)) we obtain

$$\begin{aligned} \alpha_{n,k} &= \frac{\kappa_{n+1}^{k+1}}{\kappa_n^{k+1}} \frac{\kappa_{k(n+1)+n}}{\kappa_{(k+1)(n+1)}} \frac{(n+1-k)!\, \kappa_{n-k+1}}{(n+1)!\, \kappa_{n+1}} \frac{\kappa_{n-k}}{\kappa_n} \\ &= \frac{(n+1-k)!}{\pi^{k/2}(n+1)!} \left(\frac{\Gamma\left(\frac{1}{2}n+1\right)}{\Gamma\left(\frac{1}{2}(n+1)+1\right)}\right)^{k+1} \\ &\times \frac{\Gamma\left(\frac{1}{2}(k+1)(n+1)+1\right)}{\Gamma\left(\frac{1}{2}\left((k+1)n+k\right)+1\right)} \frac{\Gamma\left(\frac{1}{2}(n+1)+1\right)}{\Gamma\left(\frac{1}{2}(n-k+1)+1\right)} \frac{\Gamma\left(\frac{1}{2}n+1\right)}{\Gamma\left(\frac{1}{2}(n-k)+1\right)}. \end{aligned}$$

Using Legendre's duplication formula for the Gamma function

$$\Gamma(z)\, \Gamma\left(z+\frac{1}{2}\right) = 2^{1-2z}\, \pi^{1/2}\, \Gamma(2z),$$

the recursion $\Gamma(1+z) = z\,\Gamma(z)$, and the fact that $k, n \in \mathbb{Z}$ we obtain

$$\begin{aligned}
\alpha_{n,k} &= \frac{(n-k)!}{\pi^{k/2} n!} \frac{\Gamma\left(\frac{1}{2}(k+1)(n+1)+1\right)}{\Gamma\left(\frac{1}{2}\left((k+1)n+k\right)+1\right)} \frac{\Gamma\left(\frac{1}{2}n+\frac{1}{2}\right)\Gamma\left(\frac{1}{2}n+1\right)}{\Gamma\left(\frac{1}{2}(n-k)+\frac{1}{2}\right)\Gamma\left(\frac{1}{2}(n-k)+1\right)} \\
&\quad \times \left(\frac{\Gamma\left(\frac{1}{2}n+1\right)}{\Gamma\left(\frac{1}{2}(n+1)+1\right)}\right)^{k+1} \\
&= \frac{1}{(2\sqrt{\pi})^k} \frac{\Gamma\left(\frac{1}{2}(k+1)(n+1)+1\right)}{\Gamma\left(\frac{1}{2}\left((k+1)n+k\right)+1\right)} \left(\frac{\Gamma\left(\frac{1}{2}n+1\right)}{\Gamma\left(\frac{1}{2}(n+1)+1\right)}\right)^{k+1} \\
&= \frac{1}{(2\sqrt{\pi})^k} \frac{\left(\Gamma\left(\frac{1}{2}n+1\right)\Gamma\left(\frac{1}{2}n+1+\frac{1}{2}\right)\right)^{k+1}}{\Gamma\left(\frac{1}{2}\left(kn+n+k\right)+1\right)\Gamma\left(\frac{1}{2}(kn+k+n)+1+\frac{1}{2}\right)} \left(\frac{\kappa_{n+1}^{k+1}}{\kappa_{(n+1)(k+1)}}\right)^2 \\
&= \frac{1}{2^k} \frac{((n+1)!)^{k+1}}{((n+1)(k+1))!} \left(\frac{\kappa_{n+1}^{k+1}}{\kappa_{(n+1)(k+1)}}\right)^2.
\end{aligned}$$

4.5 Proofs: Part II

4.5.1 Proof of Theorem 4.3.1

Let us consider the expression

$$\begin{aligned}
J &:= \int_{\mathcal{E}^{k+1}} \Delta_k(\mathbf{x}_0, \dots, \mathbf{x}_k)^p \, \mathrm{d}\mathbf{x}_0 \dots \mathrm{d}\mathbf{x}_k \\
&= \int_{(\mathbb{R}^n)^{k+1}} \Delta_k(\mathbf{x}_0, \dots, \mathbf{x}_k)^p \prod_{i=0}^{k} \mathbb{1}_{\mathcal{E}}(\mathbf{x}_i) \, \mathrm{d}\mathbf{x}_0 \dots \mathrm{d}\mathbf{x}_k.
\end{aligned}$$

Using the affine Blaschke-Petkantschin formula (see (C.2.3)) with

$$h(\mathbf{x}_0, \dots, \mathbf{x}_k) := \Delta_k(\mathbf{x}_0, \dots, \mathbf{x}_k)^p \prod_{i=0}^{k} \mathbb{1}_{\mathcal{E}}(\mathbf{x}_i)$$

yields the following representation

$$\begin{aligned}
J &= b_{n,k}(k!)^{n-k} \int_{A_{n,k}} \int_{E^{k+1}} \Delta_k(\mathbf{x}_0, \dots, \mathbf{x}_k)^{p+n-k} \prod_{i=0}^{k} \mathbb{1}_{\mathcal{E}}(\mathbf{x}_i) \, \lambda_E(\mathrm{d}\mathbf{x}_0) \dots \lambda_E(\mathrm{d}\mathbf{x}_k) \, \mu_{n,k}(\mathrm{d}E) \\
&= b_{n,k}(k!)^{n-k} \int_{A_{n,k}} \int_{(E \cap \mathcal{E})^{k+1}} \Delta_k(\mathbf{x}_0, \dots, \mathbf{x}_k)^{p+n-k} \, \lambda_E(\mathrm{d}\mathbf{x}_0) \dots \lambda_E(\mathrm{d}\mathbf{x}_k) \, \mu_{n,k}(\mathrm{d}E).
\end{aligned}$$

Now fix some $E \in A_{n,k}$. Applying Theorem 4.2.1 to the ellipsoid $\mathcal{E} \cap E$ gives

$$\begin{aligned}
&\frac{1}{\mathrm{vol}\,(\mathcal{E} \cap E)^{k+1}} \int_{(E \cap \mathcal{E})^{k+1}} \Delta_k(\mathbf{x}_0, \dots, \mathbf{x}_k)^{p+n-k} \, \lambda_E(\mathrm{d}\mathbf{x}_0) \dots \lambda_E(\mathrm{d}\mathbf{x}_k) \\
&\qquad = \frac{1}{(k!)^{p+n-k}} \frac{\kappa_{n+p}^{k+1}}{\kappa_k^{p+n+1}} \frac{\kappa_{k(n+p)+k}}{\kappa_{(k+1)(n+p)}} \frac{b_{k,k}}{b_{n+p,k}} \, \mathrm{vol}\,(\mathcal{E} \cap E)^{p+n-k},
\end{aligned}$$

which leads to

$$J = \frac{1}{(k!)^p} \frac{\kappa_{n+p}^{k+1}}{\kappa_k^{p+n+1}} \frac{\kappa_{k(n+p)+k}}{\kappa_{(k+1)(n+p)}} \frac{b_{n,k}}{b_{n+p,k}} \int\limits_{A_{n,k}} \mathrm{vol}\,(\mathcal{E} \cap E)^{p+n+1}\, \mu_{n,k}(\mathrm{d}E).$$

4.5.2 Proof of Theorem 4.3.3

The proof is similar to the previous one. Let us consider the expression

$$\begin{aligned} J :&= \int\limits_{\mathcal{E}^k} \Delta_k(0, \mathbf{x}_1, \dots, \mathbf{x}_k)^p \, \mathrm{d}\mathbf{x}_1 \dots \mathrm{d}\mathbf{x}_k \\ &= \int\limits_{(\mathbb{R}^n)^k} \Delta_k(0, \mathbf{x}_1, \dots, \mathbf{x}_k)^p \prod_{i=1}^k \mathbb{1}_{\mathcal{E}}(\mathbf{x}_i) \, \mathrm{d}\mathbf{x}_1 \dots \mathrm{d}\mathbf{x}_k. \end{aligned}$$

Using the linear Blaschke-Petkantschin formula (see (C.2.2)) with

$$h(\mathbf{x}_1, \dots, \mathbf{x}_k) := \Delta_k(0, \mathbf{x}_1, \dots, \mathbf{x}_k)^p \prod_{i=1}^k \mathbb{1}_{\mathcal{E}}(\mathbf{x}_i)$$

gives

$$\begin{aligned} J &= b_{n,k}(k!)^{n-k} \int\limits_{G_{n,k}} \int\limits_{L^k} \Delta_k(0, \mathbf{x}_1, \dots, \mathbf{x}_k)^{p+n-k} \\ &\quad \times \prod_{i=1}^k \mathbb{1}_{\mathcal{E}}(\mathbf{x}_i) \, \lambda_L(\mathrm{d}\mathbf{x}_1) \dots \lambda_L(\mathrm{d}\mathbf{x}_k) \, \nu_{n,k}(\mathrm{d}L) \\ &= b_{n,k}(k!)^{n-k} \int\limits_{G_{n,k}} \int\limits_{(L \cap \mathcal{E})^k} \Delta_k(0, \mathbf{x}_1, \dots, \mathbf{x}_k)^{p+n-k} \, \lambda_L(\mathrm{d}\mathbf{x}_1) \dots \lambda_L(\mathrm{d}\mathbf{x}_k) \, \nu_{n,k}(\mathrm{d}L). \end{aligned} \tag{4.5.1}$$

Fix some $L \in G_{n,k}$. Since $\mathcal{E} \cap L$ is an ellipsoid, there exists a linear transformation $A_L : L \to \mathbb{R}^k$ such that $A_L(\mathcal{E} \cap L) = \mathbb{B}^k$. Applying the coordinate transformation $\mathbf{x}_i = A_L \mathbf{y}_i$, $i = 1, 2, \dots, k$, we get

$$\begin{aligned} &\int\limits_{(L \cap \mathcal{E})^k} \Delta_k(0, \mathbf{x}_1, \dots, \mathbf{x}_k)^{p+n-k} \, \lambda_L(\mathrm{d}\mathbf{x}_1) \dots \lambda_L(\mathrm{d}\mathbf{x}_k) \\ &\qquad = \frac{\mathrm{vol}\,(\mathcal{E} \cap L)^{p+n}}{\kappa_k^{p+n}} \int\limits_{(\mathbb{B}^k)^k} \Delta_k(0, \mathbf{y}_1, \dots, \mathbf{y}_k)^{p+n-k} \, \mathrm{d}\mathbf{y}_1 \dots \mathrm{d}\mathbf{y}_k. \end{aligned} \tag{4.5.2}$$

It is known (see, e.g., [59, Theorem 8.2.2]) that

$$\int\limits_{(\mathbb{B}^k)^k} \Delta_k(0, \mathbf{y}_1, \dots, \mathbf{y}_k)^{p+n-k} \, \mathrm{d}\mathbf{y}_1 \dots \mathrm{d}\mathbf{y}_k = (k!)^{-p-n+k} \, \kappa_{n+p}^k \, \frac{b_{k,k}}{b_{n+p,k}}. \tag{4.5.3}$$

Substituting (4.5.3) and (4.5.2) into (4.5.1) finishes the proof.

Appendix A

Some Results From Number Theory and Geometry of Numbers

A.1 Number Theory

In this section we recall some definitions from algebra and number theory and introduce necessary technical lemmas.

A.1.1 Definitions

Definition A.1.1. *A non-constant polynomial P is **irreducible over the field** $\mathbb{F}$ if its coefficients belong to $\mathbb{F}$ and it can not be factored into the product of two non-constant polynomials with coefficients in $\mathbb{F}$.*

In this thesis we will consider only the case $\mathbb{F} = \mathbb{Q}$ and polynomials with rational coefficients $P \in \mathbb{Q}[t]$.

Definition A.1.2. *A non-constant polynomial P is **monic** if its leading coefficient is equal to 1.*

Definition A.1.3. *A non-constant polynomial $P(t)$ of degree n is **reciprocal** if it satisfies $t^n P(1/t) \equiv \pm P(t)$.*

Definition A.1.4. *Let $P(t) = a_n t^t + \ldots + a_0 \in \mathbb{Z}[t]$. The greatest common divisor of the coefficients $a_0, \ldots, a_n$ is called the **content** of P and denoted by $\mathrm{cont}(P)$.*

Definition A.1.5. *A polynomial is **primitive** if its content is equal to 1.*

Definition A.1.6. *The **'naïve' height** of the polynomial $P(t) = a_n t^t + \ldots + a_0$ is the value $H(P) = \max\limits_{0 \le i \le n} |a_i|$.*

Definition A.1.7. *Given the vector $\mathbf{w} = (w_0, \ldots, w_n)$ of positive weights we define the **weighted** l_p **height** of the polynomial $P(t) = a_n t^t + \ldots + a_0$ as follows*

$$h_{p,\mathbf{w}}(P) := \begin{cases} \left(\sum\limits_{i=0}^{n} |w_i \, a_i|^p \right)^{1/p}, & p < \infty; \\ \max\limits_{0 \le i \le n} w_i \, |a_i|, & p = \infty. \end{cases}$$

Note, that for $\mathbf{w}^1 = (1, \ldots, 1)$ and $p = \infty$ we have $h_{\infty,\mathbf{w}^1}(P) = H(P)$.

Definition A.1.8. *A number α is called an **algebraic number** if there exists an irreducible over the $\mathbb{Q}$ primitive polynomial $P \in \mathbb{Z}[t]$ such that $P(\alpha) = 0$. The polynomial defined above is unique for any algebraic number α and it is called the **minimal polynomial** of algebraic number α.*

Definition A.1.9. *The algebraic number α is called an **algebraic integer** if its minimal polynomial $P \in \mathbb{Z}[t]$ is monic.*
Definition A.1.10. *Two algebraic numbers are called **algebraic conjugates** if they have the same minimal polynomial.*
Definition A.1.11. *The **degree** of algebraic number α is degree of its minimal polynomial* $\deg(\alpha) = \deg P$.

We will denote the field of algebraic numbers by $\mathbb{A}$ and the set of algebraic numbers of degree $n \in \mathbb{N}$ by $\mathbb{A}_n$.
Definition A.1.12. ***Height function** is the function $h : \mathbb{A} \to \mathbb{R}_+$ such that for any $n \in \mathbb{N}$ and $Q > 0$ there are only finitely many algebraic numbers $\alpha \in \mathbb{A}_n$ with $h(\alpha) \le Q$ and for any algebraic conjugates α' and α we have $h(\alpha') = h(\alpha)$.*
Definition A.1.13. *Let Γ be a countable set of real numbers and $N : \Gamma \to \mathbb{R}^+$ be a positive-valued function. The pair (Γ, N) is called a **regular system** if there exists a constant $C = C(\Gamma, N) > 0$ such that for every interval $I \subset \mathbb{R}$ the following property is satisfied: for a sufficiently large number $T_0 = T_0(\Gamma, N, I) > 0$ and an arbitrary integer $T > T_0$ there exist $\gamma_1, \gamma_2, \dots, \gamma_t \in \Gamma \cap I$ satisfying*

$$\begin{aligned} &1) \quad N(\gamma_i) \le T, \qquad 1 \le i \le t, \\ &2) \quad |\gamma_i - \gamma_j| > T^{-1}, \qquad 1 \le i < j \le t, \\ &3) \quad t > C\,T|I|. \end{aligned}$$

A.1.2 Lemmas

For a polynomial P with roots $\alpha_1, \alpha_2, \dots, \alpha_n$ define the following set

$$S(\alpha_i) := \left\{ x \in \mathbb{R} : |x - \alpha_i| = \min_{1 \le j \le n} |x - \alpha_j| \right\}.$$

Assume that the roots of the polynomial P are sorted by distance from $\alpha_i = \alpha_{i,1}$

$$|\alpha_{i,1} - \alpha_{i,2}| \le |\alpha_{i,1} - \alpha_{i,3}| \le \ldots \le |\alpha_{i,1} - \alpha_{i,n}|.$$

Lemma A.1.14. *Let $x \in S(\alpha_i)$. Then*

$$|x - \alpha_i| \le n \cdot \frac{|P(x)|}{|P'(x)|}, \tag{A.1.1}$$

$$|x - \alpha_i| \le 2^{n-1} \cdot \frac{|P(x)|}{|P'(\alpha_i)|}, \tag{A.1.2}$$

$$|x - \alpha_i| \le \min_{1 \le j \le n} \left(2^{n-j} \frac{|P(x)|}{|P'(\alpha_i)|} |\alpha_i - \alpha_{i,2}| \dots |\alpha_i - \alpha_{i,j}| \right)^{1/j}. \tag{A.1.3}$$

Proof. Considering the polynomial P and its derivative P' at the point x we get

$$|P'(x)||P(x)|^{-1} \le \sum_{i=1}^{n} |x - \alpha_i|^{-1} \le n|x - \alpha_1|^{-1},$$

which establishes the first inequality.

For a proof of the second and the third inequalities see [62], [10]. □

Lemma A.1.15. *Let I be an interval, and let $A \subset I$ be a measurable set with $\mu_1 A \geq \frac{1}{2}\mu_1 I$. If for some $\delta, v > 0$, some polynomial $P \in \mathbb{Z}[t]$ of degree n and all $x \in A$ the inequality $|P(x)| < \delta\, Q^{-v}$ holds, then for all points $x \in I$ we have*

$$|P(x)| < 6^n (n+1)^{n+1} \delta\, Q^{-v}.$$

The proof of this lemma can be found in [9].

Lemma A.1.16. *Let δ, η_1, η_2 be real positive numbers, and let $P_1, P_2 \in \mathbb{Z}[t]$ polynomials without common roots of degrees at most n such that*

$$\max\left(H(P_1), H(P_2)\right) < K,$$

for some $K > K_0(\delta)$. Let $J_1, J_2 \subset \mathbb{R}$ be intervals of sizes $\mu J_1 = K^{-\eta_1}$, $\mu J_2 = K^{-\eta_2}$. If for some $\tau_1, \tau_2 > 0$ and for all $(x_1, x_2) \in J_1 \times J_2$, the inequalities

$$\max\left(|P_1(x_i)|, |P_2(x_i)|\right) < K^{-\tau_i}, \quad i = 1, 2,$$

hold, then

$$M_{\boldsymbol{\tau},\boldsymbol{\eta}} := \tau_1 + \tau_2 + 2 + 2\max(\tau_1 + 1 - \eta_1, 0) + 2\max(\tau_2 + 1 - \eta_2, 0) < 2n + \delta. \quad \text{(A.1.4)}$$

The proof of this lemma can be found in [53].

Lemma A.1.17. *For any $P_1, P_2 \in \mathbb{Z}[t]$ of degrees $n_2 = \deg P_2 \geq \deg P_1 = n_1 > 0$ we have*

$$\left(2^{n_1+n_2-2}\sqrt{n_1+n_2+1}\right)^{-1} H(P_1)\, H(P_2) \leq H(P_1 P_2) \leq (1+n_1)\, H(P_1)\, H(P_2). \quad \text{(A.1.5)}$$

For the proof see e.g. [54, Theorem 4.2.2].

Lemma A.1.18. *For any subset of roots $\alpha_{i_1}, \dots, \alpha_{i_s}$, $1 \leq s \leq n$, of the polynomial $P(t) \in \mathbb{Z}[t]$ of degree n and with leading coefficient a_n we have*

$$\prod_{j=1}^{s} |\alpha_{i_j}| \leq (n+1) 2^n\, H(P) \cdot |a_n|^{-1}.$$

The proof can be found in [29].

Lemma A.1.19 (Bertrand postulate)**.** *For any integer $n \geq 2$ there exists a prime p such that $n < p < 2n$.*

Proved by P. Chebyshev in 1850 (see for instance [52, Theorem 2.4]).

Lemma A.1.20 (Eisenstein criterion). *Let $P(t) = a_n t^n + \ldots + a_1 t + a_0$ be a polynomial with integer coefficients. If there exists a prime number p such that:*

$$\begin{cases} a_n \not\equiv 0 \mod p, \\ a_i \equiv 0 \mod p, \quad i = 0, \ldots, n-1 \\ a_0 \not\equiv 0 \mod p^2, \end{cases} \tag{A.1.6}$$

then P is irreducible over the $\mathbb{Q}$.

For a proof see [27].

A.2 Geometry of Numbers

Definition A.2.1. *Let $\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_n$ be linearly independent points in $\mathbb{R}^n$. Then the set*

$$\Lambda := \{x \in \mathbb{R}^n \colon x = u_1\mathbf{g}_1 + \ldots + u_n\mathbf{g}_n, u_i \in \mathbb{Z}\},$$

*is called a **lattice**. The system of points $\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_n$ is called a **basis of** Λ.*

Definition A.2.2. *If Λ is a lattice and the rows of matrix G form a basis of Λ then $|\det G|$ is called the **determinant of** Λ and denoted by $\det(\Lambda)$.*

The two fundamental results in geometry of number belong to Minlowski who can be considered as the founder of this area.

Theorem A.2.3 (Minkowski's linear forms theorem). *Let Λ be an n-dimensional lattice and let $a_{i,j}$, $b_j > 0$, $1 \le i, j \le n$, be real numbers such that*

$$b_1 \cdot \ldots \cdot b_n \ge \det(\Lambda)\ |\det(a_{i,j})|\,.$$

Then there is a point $\mathbf{x} \in \Lambda$ other than zero satisfying

$$\left|\sum_{j=1}^{n} a_{1,j}x_j\right| \le b_1, \quad \left|\sum_{j=1}^{n} a_{i,j}x_j\right| < b_i, \quad 2 \le i \le n.$$

For the proof see [19, pp. 73].

Definition A.2.4. *Let K be a bounded central symmetric convex body in $\mathbb{R}^n$ and $\Lambda \in \mathbb{R}^n$ be a lattice. The **k-th successive minimum** $\tau_k = \tau_k(K, \Lambda)$ of the body K with respect to the lattice Λ is the lower bound of the numbers τ such that the body τK contains k linearly independent lattice points.*

Theorem A.2.5 (Minkowski's 2nd theorem on successive minima). *Let K be a bounded central symmetric convex body in $\mathbb{R}^n$ and let $\tau_1, \ldots, \tau_n$ be the successive minima of body K in the n-dimensional lattice Λ with determinant $\det(\Lambda)$. Then*

$$\frac{2^n}{n!}\det(\Lambda) \le \tau_1\tau_2\ldots\tau_n \operatorname{vol}(K) \le 2^n \det(\Lambda).$$

The best general references here are [19, pp. 203], [47, pp. 59].

Another important topic in geometry of numbers is counting lattice points in some bounded subset D of the Euclidean space. This problem has a numerous applications in number theory. There are a lot of results providing good estimates under some conditions for subset D (see [67] for brief review).

Definition A.2.6 ([67]). *We say that a set D is in $\mathrm{Lip}(n, M, L)$ (or of Lipschitz class (n, M, L)) if D is a subset of $\mathbb{R}^n$, and if there are M maps $\phi_1, \dots, \phi_M : [0,1]^{n-1} \to \mathbb{R}^n$ satisfying Lipschitz condition*

$$|\phi_i(\mathbf{x}) - \phi_i(\mathbf{y})| \le L\,|\mathbf{x} - \mathbf{y}|\,, \qquad \mathbf{x}, \mathbf{y} \in [0,1]^{n-1},\ i = 1, \dots, M, \tag{A.2.1}$$

such that D is covered by the images of the maps ϕ_i.

Given some bounded set $D \subset \mathbb{R}^n$ some lattice Λ in $\mathbb{R}^n$ denote by $\mu_\Lambda(D)$ the number of lattice points in D. For a real number $t > 0$ and a set $D \subset \mathbb{R}^n$ denote by

$$tD := \{t\mathbf{x} : \mathbf{x} \in D\},$$

the dilate of D by the number t.

The following theorem is stated for the sets of type tD and gives the asymptotic formula for $\mu_\Lambda(tD)$ when $t \to \infty$.

Theorem A.2.7. *Let Λ be a lattice in $\mathbb{R}^n$ and let D be a bounded set in $\mathbb{R}^n$ such that the boundary ∂D of D is in $\mathrm{Lip}(n, M, L)$. Then*

$$\mu_\Lambda(tD) = \frac{\mathrm{vol}(D)}{\det(\Lambda)}\, t^n + O\left(t^{n-1}\right),$$

where the implicit constant in the big O notation depends on n, L, M only.

For the proof see [46, Chapter VI, §2].

We will apply the Theorem A.2.7 in case $\Lambda = \mathbb{Z}^n$. Given some bounded set $D \subset \mathbb{R}^n$ denote by $\mu^*(D)$ the number of points with coprime integer coordinates in D. The following lemma provides asymptotic formula for $\mu^*(tD)$ when $t \to \infty$.

Lemma A.2.8. *Let D be a bounded set in $\mathbb{R}^n$, $n \ge 2$ such that the boundary ∂D of D is in $\mathrm{Lip}(n, M, L)$. Then*

$$\mu^*(tD) = \frac{\mathrm{vol}(D)}{\zeta(n)}\, t^n + O\left(t^{n-1} (\log t)^{\lfloor 2/n \rfloor}\right), \tag{A.2.2}$$

where the implicit constant in the big-O-notation depends on n, L, M only.

Results of this type are well-known, see for example the classical monograph by Bachmann [1, pp. 436–444] (in particular, formulas (83a) and (83b) on pages 441–442). The basic ingredient of the proof is the classical Möbius inversion formula (see [55]) and Theorem A.2.7. For the detailed proof of Lemma A.2.8, see [36].

In general it is not easy to verify that the boundary of some given set is of Lipschitz type. The following result gives one easy criteria.

Theorem A.2.9. *If $D \subset \mathbb{R}^n$ is a bounded convex set which lies in a ball of radius R, then ∂D is in* $\mathrm{Lip}(n, 1, 8n^{5/2}R)$.

The proof of this theorem can be found in [67].

Appendix B

Random polynomials

In this chapter we collect some fact connected with random polynomials, random functions and distribution of their zeroes.

Definition B.0.1 ([63]). *Let n be positive integer, let $c_0, \ldots, c_n$ be deterministic complex numbers, and let ξ (which we call the atom distribution) be a complex random variable of mean zero and finite non-zero variance. Given the coefficients $c_0, \ldots, c_n$ and atom distribution ξ, we associate the **random polynomial** $G : \mathbb{C} \to \mathbb{C}$ defined by formula*

$$G(z) := \sum_{i=0}^{n} c_i \xi_i z^i,$$

where $\xi_0, \ldots, \xi_n$ are jointly independent copies of ξ.

The definition above can be considered in a more general way, namely instead of functions $1, z, \ldots, z_n$ one can consider any collection of differentiable functions $f_0(t), \ldots, f_n(t)$ and define the random functional $F : \mathbb{C} \to \mathbb{C}$ as follows

$$F(z) := \sum_{i=0}^{n} \xi_i f_i(z). \tag{B.0.1}$$

The zeroes of random function F form the point process and the most natural way to describe the point process is via its correlation function.

Definition B.0.2 ([63]). *The **k-point correlation function** $\rho_{n,F}^{(k)} : \mathbb{C}^k \to \mathbb{R}_+$ of the set of zeroes (counting multiplicity) $\{\zeta_1, \zeta_2, \ldots\}$ of random function F is defined for any natural number k by requiring*

$$\mathbb{E}\left[\sum_{i_1,\ldots,i_k \text{ — distinct}} \varphi(\zeta_{i_1}, \ldots, \zeta_{i_k})\right] = \int_{\mathbb{C}^k} \varphi(\mathbf{z}) \rho_{n,F}^{(k)}(\mathbf{z}) d\,\mathbf{z},$$

for any continuous, compactly supported, test function $\varphi : \mathbb{C}^k \to \mathbb{R}$, with the convention $\varphi(\infty) = 0$.

The k-point correlation function does not allow us to consider real and complex zeroes separately. Moreover this function is not well-defined in case of random polynomial G with real coefficients since their zeroes are symmetric with respect to real axis and it's natural to expect some zeroes lying on real axis. Thus, k-point correlation function may become singular on the real axis. The solution of

the problem in this case is to divide the complex plane $\mathbb{C}$ into three pieces, namely $\mathbb{C} = \mathbb{C}_+ \cup \mathbb{C}_- \cup \mathbb{R}$, where $\mathbb{C}_+ := \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$ is the upper half-plane and $\mathbb{C}_+ := \{z \in \mathbb{C} : \operatorname{Im} z < 0\}$ is the lower half-plane, and define the mixed (k,l)-point correlation function.

Definition B.0.3 ([63]). *For any natural numbers $k, l \geq 0$, $1 \leq k+2l$ we define the **mixed (k,l)-point correlation function** $\rho_{n,F}^{(k,l)} : \mathbb{R}^k \times (\mathbb{C}_+ \cup \mathbb{C}_-)^l \to \mathbb{R}_+$ of the set of zeroes (counting multiplicity) of random function F to be the function defined by formula*

$$\mathbb{E}\left[\sum_{\substack{i_1,\dots,i_k \text{ — distinct} \\ j_1,\dots,j_l \text{ — distinct}}} \varphi(\zeta_{i_1},\dots,\zeta_{i_k},\bar{\zeta}_{j_1},\dots,\bar{\zeta}_{j_l})\right] = \int\limits_{\mathbb{R}^k}\int\limits_{(\mathbb{C}_+\cup\mathbb{C}_-)^l} \varphi(\mathbf{x},\mathbf{z})\rho_{n,F}^{(k,l)}(\mathbf{x},\mathbf{z})d\,\mathbf{x}d\,\mathbf{z},$$

for any continuous, compactly supported, test function $\varphi : \mathbb{R}^k \times \mathbb{C}^k \to \mathbb{R}$, where ζ_i runs over an arbitrary enumeration of the real zeroes of F and $\bar{\zeta}_j$ runs over an arbitrary enumeration of the zeroes of F in $\mathbb{C}_+ \cup \mathbb{C}_-$.

It is clear that due to symmetry in case of random polynomials G we can restrict ourselves to the consideration of the zeroes in $\mathbb{R}$ and $\mathbb{C}_+$ only.

Lemma B.0.4. *Let $\mathbf{v}(t) = (f_0(t),\dots,f_n(t))^\top$ be any collection of differentiable functions and $\xi_0,\dots,\xi_n$ be elements of multivariate normal distribution with mean zero and covariance matrix C. The expected number of real zeroes on an interval (or measurable set) I of the random function $F(t)$, defined by (B.0.1) is*

$$\int\limits_I \rho_{n,F}^{(1,0)}(t)\,dt,$$

where

$$\rho_{n,F}^{(1,0)}(t) = \frac{1}{\pi}\left[\frac{\partial^2}{\partial x \partial y}\log\left(\mathbf{v}(x)^\top C\,\mathbf{v}(y)\right)\Big|_{x=y=t}\right]^{1/2}. \tag{B.0.2}$$

For the proof see [26].

The following lemma gives the representation of random vector $\boldsymbol{\xi}$ having uniform distribution in the $(n+1)$-dimensional unit ball in terms of independent random variables.

Lemma B.0.5. *Let $\eta_0,\eta_1,\dots,\eta_n$ be i.i.d. standard Gaussian random variables, and let Z be an exponential random variable independent of $\eta_0,\eta_1,\dots,\eta_n$. Then the random vector*

$$\boldsymbol{\xi} := \frac{(\eta_0,\eta_1,\dots,\eta_n)}{\sqrt{\sum\limits_{i=0}^{n}|\eta_i|^2 + Z}}$$

has the uniform distribution on the $(n+1)$-dimensional unit ball.

This lemma is the special case of the more general result [4, Theorem 1, $p = 2$].

Appendix C

Integral Geometry

In this chapter we introduce some basic notions of integral geometry following [59].

For $p > 0$ we write

$$\kappa_p := \frac{\pi^{p/2}}{\Gamma\left(\frac{p}{2}+1\right)}, \tag{C.0.1}$$

where for an integer k we have $\kappa_k = \mathrm{vol}\left(\mathbb{B}^k\right)$, and for any real $p > 0$ and any real number $q > p-1$ we write

$$b_{q,p} := \frac{\omega_{q-p+1}\dots\omega_q}{\omega_1\cdots\omega_p} \tag{C.0.2}$$

with $\omega_k := k\kappa_k$ being equal to the area of unit $(k-1)$-dimensional sphere for an integer k.

Definition C.0.1. *For $k \in \{0,\dots,n\}$, let $G_{n,k}$ be the set of all k-dimensional linear subspaces of $\mathbb{R}^n$, and let $A_{n,k}$ be the set of all k-dimensional affine subspaces of $\mathbb{R}^n$. The sets $G_{n,k}$ and $A_{n,k}$ can be endowed with the finest topologies (see [59, Section 13.2] for more details). Thus the topological spaces $G_{n,k}$ are called **linear Grassmannians** and the topological spaces $A_{n,k}$ are called **affine Grassmannians**.*

According to [59, Theorem 13.2.11], there is a unique rotation invariant Haar measure $\nu_{n,k}$ on $G_{n,k}$, normalized by

$$\nu_{n,k}(G_{n,k}) = 1,$$

and, according to [59, Theorem 13.2.12], there is a unique rigid motion invariant Haar measure $\mu_{n,k}$ on $A_{n,k}$, normalized by

$$\mu_{n,k}\left(\{E \in A_{n,k} : E \cap \mathbb{B}^n \neq \emptyset\}\right) = \kappa_{n-k}.$$

For any linear subspace $L \in G_{d,k}$ we denote by λ_L the k-dimensional Lebesgue measures on L and for any affine subspace $E \in A_{d,k}$ we denote by λ_E the k-dimensional Lebesgue measures on E. The Lebesgue measure on $\mathbb{R}^n$ is denoted by λ_n.

Definition C.0.2. *By a **convex body** in $\mathbb{R}^n$ we understand a compact convex subset of $\mathbb{R}^n$ with non-empty interior.*

Definition C.0.3. *Given a subset $S \subset \mathbb{R}^n$ and a point $x \in \mathbb{R}^n$ we define by*

$$d(x,S) := \inf_{s\in S} \|x-s\|_2$$

*the **distance between the point and the set**.*

Definition C.0.4. *For k-dimensional subspace $L \subset \mathbb{R}^n$, $k \leq n$ denote by $P_L : \mathbb{R}^n \to L$ the* ***orthogonal projection operator****:*

$$P_L(x) := d(x, L).$$

Definition C.0.5. *The* ***linear hull (span)*** *of a set $X \subset \mathbb{R}^n$ is the smallest linear subspace of $\mathbb{R}^n$ that contains X and is denoted by $\operatorname{span}(X)$. If the set X consists of the finite number of points $X = \{x_1, \ldots, x_m\}$ then the linear hull of X can be also defined as the following set*

$$\operatorname{span}(X) = \operatorname{span}(x_1, \ldots, x_m) = \left\{ \sum_{i=1}^{m} \lambda_i x_i \colon \lambda_i \in \mathbb{R} \right\}.$$

Definition C.0.6. *The* ***convex hull*** *of a set $X \subset \mathbb{R}^n$ is the smallest convex set that contains X and is denoted by $\operatorname{conv}(X)$. If the set X consists of the finite number of points $X = \{x_1, \ldots, x_m\}$ then the convex hull of X can be also defined as the following set*

$$\operatorname{conv}(X) = \operatorname{conv}(x_1, \ldots, x_m) = \left\{ \sum_{i=1}^{m} \lambda_i x_i \colon \lambda_i \geq 0, \sum_{i=1}^{m} \lambda_i = 1 \right\}.$$

Definition C.0.7. *The n-dimensional* ***simplex*** *is the n-dimensional polytope which is the convex hull of $n+1$ points in $\mathbb{R}^m$, $n \leq m$ (vertices of the simplex).*

Definition C.0.8. *For subsets $A, B \subset \mathbb{R}^n$, the set $A + B := \{a + b \colon a \in A, b \in B\}$ is the* ***Minkowski sum*** *of the sets A and B.*

Definition C.0.9. *For convex body $K \subset \mathbb{R}^n$ and $\epsilon > 0$, the set*

$$K_\epsilon := K + \epsilon \mathbb{B}^n = \{\mathbf{x} \in \mathbb{R}^n \colon d(\mathbf{x}, K) \leq \epsilon\}$$

is the ***parallel body*** *of K at distance ϵ.*

C.1 Intrinsic Volumes

The concept of intrinsic volumes is an important characteristic of the convex sets. In this section we introduce the definition of intrinsic volumes and some important properties. For more details we refer the reader to [59, Section 14.2].

Given some convex set $K \subset \mathbb{R}^n$ consider its parallel body K_ϵ. It is an interesting fact that the volume of K_ϵ is a polynomial in ϵ of degree at most n. This result is known as the **Steiner formula** and can be written as follows

$$\operatorname{vol}(K_\epsilon) = \sum_{k=0}^{n} \epsilon^{n-k} \kappa_{n-k} V_k(K).$$

The functionals $V_0, \ldots, V_n$ are called the **intrinsic volumes**. Due to the normalization $V_k(K)$ depends only on K and not on the dimension of its surrounding space.

In general it is very difficult task to derive the good representation for the intrinsic volumes $V_k(K)$. One of the representations, known as Kubota's formula, is very useful:

$$V_k(K) = \binom{n}{k} \frac{\kappa_n}{\kappa_k \kappa_{n-k}} \int\limits_{G_{n,k}} \mathrm{vol}(P_L K)\, \nu_{n,k}(dL). \tag{C.1.1}$$

It should be noted that some intrinsic volumes have the geometric meaning. For example, $V_n(K)$ is equal to n-dimensional volume, $2V_{n-1}(K)$ is equal to surface area and $\frac{2\kappa_{n-1}}{d\kappa_n} V_1(K)$ is equal to mean width of the body K.

C.2 Blaschke-Petkantschin Formulas

In this section we will introduce such powerful tool as Blaschke-Petkantschin formulas.

For $k \in \{0, \dots, n\}$ and $\mathbf{x}_1, \dots, \mathbf{x}_k \in \mathbb{R}^n$ we denote by $\nabla_k(\mathbf{x}_1, \dots, \mathbf{x}_k)$ the k-dimensional volume of the parallelepiped spanned by the vectors $\mathbf{x}_1, \dots, \mathbf{x}_k$. For $k+1$ points $\mathbf{x}_0, \dots, \mathbf{x}_k \in \mathbb{R}^n$ we denote by

$$\Delta_q(\mathbf{x}_0, \dots, \mathbf{x}_k) := \mathrm{vol}\left(\mathrm{conv}(\mathbf{x}_0, \dots, \mathbf{x}_k)\right)$$

the k-dimensional volume of the convex hull of $\mathbf{x}_0, \dots, \mathbf{x}_k$. Moreover the following equality holds for any $\mathbf{x}_0, \dots, \mathbf{x}_k \in \mathbb{R}^n$:

$$\Delta_q(\mathbf{x}_0, \dots, \mathbf{x}_k) = \frac{1}{k!} \nabla_k(\mathbf{x}_1 - \mathbf{x}_0, \dots, \mathbf{x}_k - \mathbf{x}_0). \tag{C.2.1}$$

It is typical situation in the area of Integral Geometry when one needs to integrate some non-negative measurable function $h : (\mathbb{R}^n)^k \to \mathbb{R}_+$ with respect to product measure λ_n^k. To this end, we integrate first over the k-tuples of points in a fixed k-dimensional linear subspace L, with respect to the product measure λ_L^k, and then integrate over $G_{n,k}$, with respect to $\nu_{n,k}$. The corresponding transformation formula is known as the linear Blaschke-Petkantschin formula (see [59, Theorem 7.2.1]):

$$\int\limits_{(\mathbb{R}^n)^k} h(\mathbf{x}_1, \dots, \mathbf{x}_k)\, \mathrm{d}\mathbf{x}_1 \dots \mathrm{d}\mathbf{x}_k = b_{n,k}(k!)^{n-k} \int\limits_{G_{n,k}} \int\limits_{L^k} h(\mathbf{x}_1, \dots, \mathbf{x}_k) \tag{C.2.2}$$
$$\times \Delta_k(0, \mathbf{x}_1, \dots, \mathbf{x}_k)^{n-k}\, \lambda_L(\mathrm{d}\mathbf{x}_1) \dots \lambda_L(\mathrm{d}\mathbf{x}_k)\, \nu_{n,k}(\mathrm{d}L),$$

where $b_{n,k}$ is defined in (C.0.2).

A similar affine version (see [59, Theorem 7.2.7]) may be stated as follows:

$$\int\limits_{(\mathbb{R}^n)^{k+1}} h(\mathbf{x}_0, \dots, \mathbf{x}_k)\, \mathrm{d}\mathbf{x}_0 \dots \mathrm{d}\mathbf{x}_k = b_{n,k}(k!)^{n-k} \int\limits_{A_{n,k}} \int\limits_{E^{k+1}} h(\mathbf{x}_0, \dots, \mathbf{x}_k) \tag{C.2.3}$$
$$\times \Delta_k(\mathbf{x}_0, \dots, \mathbf{x}_k)^{n-k}\, \lambda_E(\mathrm{d}\mathbf{x}_0) \dots \lambda_E(\mathrm{d}\mathbf{x}_k)\, \mu_{n,k}(\mathrm{d}E).$$

C.3 Ellipsoids

Any non-degenerate centered ellipsoid $\mathcal{E} \subset \mathbb{R}^n$ is defined by some unique symmetric positive-definite $n \times n$ matrix H as

$$\mathcal{E} = \left\{ \mathbf{x} \in \mathbb{R}^n \colon \sqrt{\mathbf{x}^\top H^{-1} \mathbf{x}} \leq 1 \right\}. \tag{C.3.1}$$

The volume of $\mathcal{E}$ is given by $\sqrt{\det H} \cdot \mathrm{vol}(\mathbb{B}^n)$ and the formulas for the intrinsic volumes can be found in [68].

Since H is symmetric positive-definite, there exists a unique symmetric positive-definite $n \times n$ matrix A (called a square root of H) such that $H = A^2$ (see, e.g., [40, Theorem 7.2.6]). Hence (C.3.1) is equivalent to

$$\mathcal{E} = A\mathbb{B}^n := \left\{ \mathbf{x} \in \mathbb{R}^n \colon \sqrt{\mathbf{x}^\top A^{-2} \mathbf{x}} = \|A^{-1}\mathbf{x}\| \leq 1 \right\}.$$

Bibliography

[1] P. Bachmann. *Die Analytische Zahlentheorie*. Nabu Press, 2010. 103

[2] A. Baker and W. M. Schmidt. Diophantine approximation and Hausdorff dimension. *Proceedings of the London Mathematical Society*, 21(3):1–11, 1970. 31, 32

[3] F. Barroero and M. Widmer. Counting lattice points and O-minimal structures. *International Mathematics Research Notices*, 2014(18):4932–4957, 2014. 11

[4] F. Barthe, O. Guédon, S. Mendelson, and A. Naor. A probabilistic approach to the geometry of the l_p^n-ball. *The Annals of Probability*, 33(2):480–513, 2005. 106

[5] U. Bäsel. Random chords and point distances in regular polygons. *Acta Mathematica Universitatis Comenianae*, 83(1):1–18, 2014. 87

[6] V. Beresnevich. Effective measure estimates for sets of real numbers with a given error of approximation by quadratic irrationalities. *Vestsi Akad. Navuk Belarusi Ser. Fiz. Mat. Navuk*, (4):10–15, 1996. 32

[7] V. Beresnevich. On approximation of real numbers by real algebraic numbers. *Acta Arithmetica*, 90(2):97–112, 1999. 31, 32

[8] V. Beresnevich, D. Dickinson, and S. Velani. Diophantine approximation on planar curves and the distribution of rational points. *Annals of Mathematics*, 166(2):367–426, 2007. 5, 66

[9] V. Bernik. A metric theorem on the simultaneous approximation of zero by values of integer polynomials. *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya*, 44(1):24–45, 1980. 101

[10] V. Bernik. Application of the Hausdorff dimension in the theory of Diophantine approximations. *Acta Arithmetica*, 42(3):219–253, 1983. 101

[11] V. Bernik, N. Budarina, and D. Dickinson. A divergent Khintchine theorem in the real, complex, and p-adic fields. *Lithuanian Mathematical Journal*, 48(2):158–173, 2008. 32

[12] V. Bernik, F.Götze, and A. Gusakova. On points with algebraically conjugate coordinates close to smooth curves. *Moskow Journal of Combinatirics and Number Theory*, 6(2—3):57—100, 2016. 5

[13] V. Bernik, F. Götze, and O. Kukso. On algebraic points in the plane near smooth curves. *Lithuanian Mathematical Journal*, 54(3):231–251, 2014. 52, 54, 66

[14] V.I. Bernik and F. Götze. Distribution of real algebraic numbers of arbitrary degree in short intervals. *Russian Academy of Sciences. Izvestiya: Mathematics*, 79(1):18–39, 2015. 32, 33, 72

[15] E. Borel. *Principes et formules classiques du calcul des probabilités*. Number 1 in Traité du calcul des probabilités et de ses applications. Gauthier-Villars, Paris, 2 edition, 1947. 87

[16] Y. Bugeaud. Approximation by algebraic integers and Hausdorff dimension. *Journal of the London Mathematical Society*, 65(3):547–559, 2002. 31

[17] Y. Bugeaud. *Approximation by algebraic numbers*. Number 160 in Cambridge tracts in mathematics. Cambridge University Press, Cambridge, 2004. 32

[18] Y. Bugeaud and M. Mignotte. On the distance between roots of integer polynomials. *Proceedings of the Edinburgh Mathematical Society*, 47(3):553–556, 2004. 33, 47, 67

[19] J. W. S. Cassels. *An Introduction to the Geometry of Numbers*. Springer, Berlin, Heidelberg, 1996. 73, 102, 103

[20] G. D. Chakerian. Inequalities for the difference body of a convex body. *Proceedings of the American Mathematical Society*, 18:879–884, 1967. 89

[21] N. Dafnis and G. Paouris. Estimates for the affine and dual affine quermassintegrals of convex bodies. *Illinois Journal of Mathematics*, 56(4):1005–1021, 2012. 86

[22] H. Davenport. On a principle of Lipschitz. *Journal of the London Mathematical Society*, 26(3):179–183, 1951. 10

[23] H. Dickinson and M. M. Dodson. Extremal manifolds and Hausdorff dimension. *Duke Mathematical Journal*, 101(2):271–281, 2000. 32

[24] A. Dubickas. Polynomials irreducible by Eisenstein's criterion. *Applicable Algebra in Engineering Communication and Computing*, 14(2):127–132, 2003. 11

[25] A. Dubickas. On the number of reducible polynomials of bounded naive height. *Manuscripta Mathematica*, 144(3-4):439–456, 2014. 11

[26] A. Edelman and E. Kostlan. How many zeros of a random polynomial are real? *Bulletin of American Mathematical Society*, 32(1):1–37, 1995. 4, 15, 106

[27] G. Eisenstein. Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt. *Journal für die reine und angewandte Mathematik*, 1850(39):160–179, 1850. 102

[28] Jan-Hendrik Evertse. Distances between the conjugates of an algebraic number. *Publicationes Mathematicae Debrecen*, 65(3–4):323–340, 2004. 33, 47, 67

[29] N. Fel'dman. The approximation of certain transcendental numbers I. Approximation of logarithms of algebraic numbers. *Izvestiya Akademii Nauk SSSR. Ser. Mat.*, 15(1):53–74, 1951. 101

[30] H. Furstenberg and I. Tzkoni. Spherical functions and integral geometry. *Israel Journal of Mathematics*, 10:327–338, 1971. iii, 84, 90

[31] B. Ghosh. Random distances within a rectangle and between two rectangles. *Bulletin of the Calcutta Mathematical Society*, 43:17–24, 1951. 87

[32] F. Götze and A. Gusakova. On algebraic integers in short intervals and near smooth curves. *Acta Arithmetica*, 179(3):251–265, 2017. 6

[33] F. Götze, A. Gusakova, Z. Kabluchko, and D. Zaporozhets. Distribution of complex algebraic numbers on the unit circle. 4

[34] F. Götze, A. Gusakova, and D. Zaporozhets. Random affine simplexes. *Journal of Applied Probability (to appear)*. 7

[35] F. Götze, D. Kaliada, and D. Zaporozhets. Correlations between real conjugate algebraic numbers. *Chebyshevskiĭ Sbornik*, 16(4):90–99, 2015. 4, 13

[36] F. Götze, D. Kaliada, and D. Zaporozhets. Distribution of complex algebraic numbers. *Proceedings of the American Mathematical Society*, 145(1):61–71, 2017. 13, 103

[37] F. Götze, D. Koleda, and D. Zaporozhets. Joint distribution of conjugate algebraic numbers: a random polynomial approach. *arXiv:1703.02289*. 13, 19

[38] J. Grote, Z. Kabluchko, and C. Thäle. Limit theorems for random simplices in high dimensions. *arXiv: 1708.00471*. 84, 88

[39] L. Heinrich. Lower and upper bounds for chord power integrals of ellipsoids. *Applied Mathematical Sciences*, 8(165):8257–8269, 2014. 88

[40] R. A. Horn and C. R. Johnson. *Matrix analysis*. Cambridge University Press, 1990. 110

[41] M. N. Huxley. *Area, Lattice Points and Exponential Sums*. Oxford University Press, 1996. 5, 66

[42] Z. Kabluchko, D. Temesvari, and C. Thäle. Expected intrinsic volumes and facet numbers of random beta-polytopes. *arXiv: 1707.02253*. 84, 87

[43] J. F. C. Kingman. Random secants of a convex body. *Journal of Applied Probability*, 6(3):660–672, 1969. 89

[44] D. Koleda. On the density function of the distribution of real algebraic numbers. *Journal de Théorie des Nombres de Bordeaux*, 29(1):179–200, 2017. 12

[45] G. Kuba. On the distribution of reducible polynomials. *Mathematica Slovaca*, 59(3):349–356, 2009. 11, 23, 24

[46] S. Lang. *Algebraic number theory.* Graduate text in mathematics 110. springer-Verlang, New York Inc., 1994. 10, 11, 103

[47] C.G. Lekkerkerker and P.M. Gruber. *Geometry of Numbers*, volume 37 of *North-Holland Mathematical Library.* North Holland, 1987. 103

[48] R. Lipschitz. Über die asymptotischen Gesetze von gewissen Gttungen zahlentheoretischer Funktionen. *Monatsber. der Berliner Akademie*, pages 174–185, 1865. 10

[49] D. Masser and J. D. Vaaler. Counting algebraic numbers with large height II. *Transactions of the American Mathematical Society*, 359(1):427–445, 2007. 10, 11

[50] A. M. Mathai. *An introduction to geometrical probability.* Number 1 in Statistical distributions and models with applications. Gordon & Breach Science Publisher, 1999. 87

[51] R. E. Miles. Isotropic random simplices. *Advances in Applied Probability*, 3(2):353–382, 1971. 83, 84, 87

[52] Y. Nesterenko. *Number theory.* Akademiya, 2008. 101

[53] N. Pereverzeva. The distribution of vectors with algebraic coordinates in $\mathbb{R}^2$. *Vestsi Akad. Naavuk BSSR. Ser. Fiz.-Mat. Navuk*, 4:114—116, 1987. 101

[54] Victor V. Prasolov. *Polynomials*, volume 11 of *Algorithms and Computation in Mathematics.* Springer-Verlag, Berlin, 2010. 75, 101

[55] H. Rademacher. *Lectures on elementary number theory.* Robert E. Krieger Publishing Co., Huntington, 1977. 10, 103

[56] H. Ruben and R.E. Miles. A canonical decomposition of the probability measure of sets of isotropic random points in $\mathbb{R}^n$. *Journal of Multivariate Analysis*, 10(1):1–18, 1980. 83

[57] L. A. Santaló. *Integral geometry and geometric probability.* Cambridge mathematical library. Cambridge University Press, Cambridge, 2004. 87

[58] W.M. Schmidt. Northcott's theorem on heights II. The quadratic case. *Acta Arithmetica*, 70(4):343–375, 1995. 10

[59] R. Schneider and W. Weil. *Stochastic and integral geometry.* Probability and its applications. Springer, Berlin, 2008. 87, 97, 107, 108, 109

[60] F. Schweppe. *Uncertain Dynamic Systems: Modelling, Estimation, Hypothesis Testing, Identification and Control.* Prentice Hall, 1973. 91

[61] P. G. Spain. Lipschitz^2: a new version of an old principle. *The Bulletin of the London Mathematical Society*, 27(6):565–566, 1995. 10

[62] V. G. Sprindzuk. *Mahler's problem in metric number theory.* Translated from the Russian by B. Volkmann. Translations of Mathematical Monographs, Vol. 25. American Mathematical Society, Providence„ 1969. 42, 46, 101

[63] T. Tao and V. Vu. Local universality of zeroes of random polynomials. *International Mathematics Research Notices*, 2015(13):5053–5139, 2015. 105, 106

[64] R. C. Vaughan and S. Velani. Diophantine approximation on planar curves: the convergence theory. *Inventiones Mathematicae*, 166(1):103–124, 2006. 5, 66

[65] B. L. Waerden. Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt. *Monatshefte für Mathematik und Physik*, 43(1):133–147, 1936. 11

[66] M. Widmer. Counting primitive points of bounded height. *Transactions of the American Mathematical Society*, 362(9):4793–4829, 2010. 10

[67] M. Widmer. Lipschitz class, narrow class and counting lattice points. *Proceedings of American Mathematical Society*, 140(2):677–689, 2012. 10, 11, 103, 104

[68] D. Zaporozhets and Z. Kabluchko. Random determinants, mixed volumes of ellipsoids, and zeros of Gaussian random fields. *Journal of Mathematical Sciences*, 199(2):168–173, 2014. 86, 110