Manfred G. Madritsch

Matrikelnummer 0130439

Exponential sums: Normal numbers and Waring's Problem

Dissertation[1]

Ausgeführt zum Zwecke der Erlangung
des akademischen Grades eines
Doktors der technischen Wissenschaften

Betreuer:

O. Univ.-Prof. Dr. Robert F. Tichy

unter Mitwirkung von

Ao. Univ.-Prof. Dr. Jörg M. Thuswaldner

Eingereicht an der Technischen Universität Graz
Fakultät für Technische Mathematik und Technische Physik

Graz, April 2008

[1]Supported by the Austrian Science Fund (FWF) FSP-Project S9603 and S9611

Preface

If $f : \mathbb{N} \to \mathbb{R}$ is a given arithmetic function then we call a sum of the form

$$\sum_{n=1}^{N} \exp(2\pi i f(n)) \tag{$*$}$$

an exponential sum. These sums are a central tool in analytic number theory and have applications in different areas such as in uniform distribution, counting zeros of ζ-functions and additive problems.

We mention the seminal paper by Weyl from 1916, where he considered the uniform distribution of sequences $(p(n))_{n\geq 1}$ where p is a polynomial. These considerations lead him to the statement of a criterion (later called Weyl's criterion) for a sequence to be uniformly distributed, saying that a sequence is uniformly distributed if and only if certain exponential sums have non-trivial estimates (*cf.* Theorem 1.3).

Weyl's results where extended by Van der Corput. He improved Weyl's method in order to estimate the Riemann zeta-function in the critical strip. In this case $f(n) = -\frac{t}{2\pi} \log n$ in $(*)$.

Another problem from the same context is the Dirichlet divisor problem. Let $d(n)$ denote the number of divisors of the number n. Then one is interested in estimates of

$$\Delta(x) = \sum_{n \leq x} d(n) - x \log x - (2\gamma - 1)x,$$

where γ is Euler's constant. These sums are estimated by a Fourier transform of the function $\psi(x) = x - \lfloor x \rfloor - \frac{1}{2}$.

Fourier transformation also plays a role in uniform distribution, especially in discrepancy theory, where one is interested in a function, that is a good approximation of an Urysohn function and which has a nice Fourier transform. These functions were introduced by Vinogradov and play a central role in the estimation of the discrepancy of normal numbers.

The exponential sums occurring in the estimation of the Urysohn function where also considered by R.C. Baker in 1984. In particular he was able to show the uniform distribution of the values of certain entire functions. This was the starting point of my research work and will be described in Chapter 2 where we want to construct normal numbers with help of entire functions of the same type as those considered by Baker. The theoretical background to the used constructions and their motivation will be presented in Chapter 1.

Chapter 3 will lead us a little bit away from the estimation of exponential sums. It contains preliminary results on normal numbers in matrix number systems that will be used later. Some of its results, however, are of interest on its own right. We consider normal numbers in different number systems, where these systems and the associated concept of normal numbers are introduced and described in Chapter 1. Moreover we show how one can extend the construction of Copeland and Erdős to matrix number systems.

In Chapter 4 we want to combine the methods used in Chapter 2 with the results of Chapter 3 in order to extend the construction by Nakai and Shiokawa to the Gaussian number systems. Therefore we have to estimate exponential sums over the Gaussian integers which are similar to the considerations of Hua and Wang, who introduced exponential sums in algebraic number fields.

Besides the construction of normal numbers and uniform distribution we are also concerned with applications of exponential sums in additive problems. The fundamental problem is to consider number of solutions of equations of the form

$$N = x_1 + \cdots + x_s \quad (x_1, \dots, x_s \in \mathcal{S}),$$

where $\mathcal{S}$ is a subset of the positive integers. Interesting choices for $\mathcal{S}$ are for instance the k-th powers, the prime numbers, the k-th powers of prime numbers, the square-free numbers, the k-free numbers. The basic tool in the estimation of the numbers of solution is the orthogonality of the exponential sums, *i.e.*,

$$\int_0^1 \exp(2\pi i\alpha n) = \begin{cases} 1 & \text{if n=0,} \\ 0 & \text{otherwise.} \end{cases}$$

Then in order to apply the circle method one has to consider sums of the form

$$\sum_{\substack{n=1 \\ n\in\mathcal{S}}}^{N} \exp(2\pi i\alpha n),$$

where α is either in a Major or in a Minor arc. For $\mathcal{S}$ equal to the set of primes or the k-th powers of primes good estimates are due to Hua and Vinogradov. For the k-free numbers Brüdern, Granville, Perelli, Vaughan, and Wooley give estimates.

In our case we want to set $\mathcal{S}$ to a digitally restricted set. This is the set where the sum of digits function of every element fulfills certain congruence relations. These sets and their additive properties have been studied by Thuswaldner and Tichy in 2005. In Chapter 5 we consider generalizations of this problem to polynomials over function fields. The corresponding results for k-th powers, irreducible polynomials in this field were gained by Car, Hayes, Kubota and Webb.

In the last Chapter I will present a recent result of a generalization of the additive problem with digital restrictions to function fields. The number systems and additive functions in this area are motivated by recent considerations of Scheicher and Thuswaldner.

I would like to thank all those, who inspired and supported my work. In particular I want to thank Robert Tichy and Jörg Thuswaldner for their useful comments and hints, my office colleagues Christoph Aistleiter, Philipp Mayer, and Stephan Wagner, for our discussions about everything under the sun. I also have to thank the Austrian Science Fund - without their support it would have been impossible to write my thesis.

Manfred Madritsch

Contents

Chapter 1

Introduction and definitions

We call a sum of the form

$$S(f, N) := \sum_{n=1}^{N} \exp(2\pi i f(n))$$

an *exponential sum* and we will write for short $e(x) := \exp(2\pi i x)$, thus

$$S(f, N) = \sum_{n=1}^{N} e(f(n)).$$

If f is a polynomial then the sum $S(f, N)$ is also called a *Weyl sum*.

Since $e(\cdot)$ is 1-periodic it suffices to consider the fractional part of a real number. We denote by $\{x\}$ the fractional part of x and by $\|x\| = \min_{n\in\mathbb{Z}} |x - n|$ the minimum distance to an integer.

If there exists a positive integer q such that $\{f(n+q)\} = \{f(n)\}$ holds for every integer n, then we call the sum

$$S_q(f) := \sum_{n=1}^{q} e(f(n))$$

a *complete exponential sum*. A simple example for a complete sum is if f is a polynomial with rational coefficients and least common denominator q, *i.e.*, then $\{f(n + q)\} = \{f(n)\}$ and

$$S_q(f) = \sum_{x=1}^{q} e\left(\frac{a_d x^d + \cdots + a_1 x + a_0}{q}\right)$$

with $a_d \not\equiv 0 \pmod{q}$.

1.1 Uniform distribution

The formal definition of uniform distribution was given by Weyl [84]. For a good survey on that topic consider the book of Kuipers and Niederreiter [47]. Another book giving a very good and more recent view on that topic is the one of Drmota and Tichy [21]. In this section we mainly follow these to books in our definitions.

Definition 1.1. We call a sequence $(x_n)_{n\geq 1}$ of real numbers *uniformly distributed modulo 1* if for every pair $0 \leq a < b \leq 1$ we have

$$\lim_{N\to\infty} \frac{|\{1 \leq n \leq N : \{x_n\} \in [a, b)\}|}{N} = b - a$$

where $|S|$ denotes the cardinality of S. This is equivalent to the following

Definition 1.2. A sequence $(x_n)_{n\geq 1}$ of real numbers is *uniformly distributed modulo 1* if for every continuous real-valued function f defined on $[0,1]$ we have

$$\lim_{N\to\infty}\sum_{n=1}^{N} f(\{x_n\}) = \int_0^1 f(x)\mathrm{d}x.$$

Now we have reached the point where exponential sums come into play. They were introduced by Weyl in [84] in order to give the following criterion.

Theorem 1.3 ([84] **Weyl's criterion**). *A sequence $(x_n)_{n\geq 1}$ is uniformly distributed modulo 1 if and only if for every non-zero integer h*

$$\sum_{n\leq N} e(h\cdot x_n) = o(N).$$

In the same paper Weyl applied this criterion to sequences

$$\left(f(n)\right)_{n\in\mathbb{N}},$$

where f is a polynomial. He was able to show, that this sequence is uniformly distributed if and only if $f - f(0)$ has at least one irrational coefficient (*cf.* Satz 9 in [84]). A weaker result (namely for $f(x) = ax^q$) was shown independently by Hardy and Littlewood [30]. In modern theory it is more convenient to prove this with Van der Corput's method which we will present in the following. We want to remark that the above result also holds if the sequence over the positive integers is replaced by the primes as Vinogradov showed [71].

1.1.1 Weyl's result

Theorem 1.4. *Let f be a polynomial with real coefficients. The sequence*

$$\left(f(n)\right)_{n\in\mathbb{N}}$$

is uniformly distributed modulo 1 if and only if $f - f(0)$ has at least one irrational coefficient.

First we consider the special case of f being linear.

Lemma 1.5. *For α a real we get that*

$$\left|\sum_{n=1}^{N} e(\alpha\, n)\right| \leq \min\left(N, \frac{1}{2\left\|\alpha\right\|}\right).$$

Proof. By estimating every $e(\alpha\, n)$ trivially we get that

$$\left|\sum_{n=1}^{N} e(\alpha\, n)\right| \leq N.$$

On the other hand

$$\left|\sum_{n=1}^{N} e(\alpha\, n)\right| = \left|\frac{e(\alpha(N+1))-1}{e(\alpha)-1}\right| \leq \frac{1}{2\sin\left(\pi\left\|\alpha\right\|\right)} \leq \frac{1}{2\left\|\alpha\right\|}$$

and the lemma follows. □

Now we show an inequality, that helps us reducing the degree of the function f by one. Therefore we introduce the difference function Δ_k for k a non-negative integer. We define Δ_k recursively by

$$\begin{aligned}\Delta_0(f(x)) &:= f(x),\\ \Delta_{k+1}(f(x); y_1,\dots,y_{k+1}) &:= \Delta_k(f(x+y_{k+1}); y_1,\dots,y_k) - \Delta_k(f(x); y_1,\dots,y_k).\end{aligned}$$

The idea behind the following lemma is often called "Weyl difference". The following inequality is due to Van der Corput.

Lemma 1.6 ([47, Theorem 3.1]). *Let $u_1, \dots, u_N$ be complex numbers, and let H be an integer with $1 \le K \le N$. Then*

$$\left| \sum_{n=1}^{N} u_n \right|^2 \le \frac{N+K-1}{K} \left(\sum_{n=1}^{N} |u_n|^2 + 2 \sum_{k=1}^{K} \left(1 - \frac{k}{K}\right) \Re \sum_{n=1}^{N-k} u_n \overline{u_{n+k}} \right),$$

where $\Re z$ denotes the real part of z.

Now one can state the following very useful theorem.

Theorem 1.7 ([47] **Van der Corput's Difference Theorem**). *Let $(x_n)_{n\ge1}$ be a sequence of real numbers. If for every positive integer h the sequence $(x_{n+h} - x_n)_{n\ge1}$ is uniformly distributed modulo 1, then $(x_n)_{n\ge1}$ is uniformly distributed modulo 1.*

Proof. By an application of Lemma 1.6 with $u_n = e(h\,x_n)$ we get that

$$\left| \frac{1}{N} \sum_{n=1}^{N} e(h\,x_n) \right|^2 \le \frac{N+K-1}{NK} \left(\frac{1}{N} \sum_{n=1}^{N} |e(h\,x_n)|^2 + \frac{2}{N} \sum_{k=1}^{K} \left(1 - \frac{k}{K}\right) \Re \sum_{n=1}^{N-k} e(h(x_n - x_{n+h})) \right). \tag{1.1.1}$$

Since $(x_{n+h} - x_n)_{n\ge1}$ is uniformly distributed modulo 1 for every positive integer h we get

$$\lim_{N\to\infty} \frac{1}{N-k} \sum_{n=1}^{N-k} e(h(x_n - x_{n+h})) = 0. \tag{1.1.2}$$

Putting (1.1.1) and (1.1.2) together we get

$$\limsup_{N\to\infty} \left| \frac{1}{N} \sum_{n=1}^{N} e(h\,x_n) \right|^2 \le \frac{1}{K}$$

for every positive integer K and the theorem follows. □

Now we are in the position to give the proof of Weyl's result.

Proof of Theorem 1.4. Let f be such that

$$f(x) = \alpha_d x^d + \cdots + \alpha_1 x + \alpha_0.$$

Necessity: Assume all coefficients are rational. Then let q be the greatest common divisor of the coefficients of f and write

$$f(x) = \frac{a_d x^d + \cdots + a_1 x}{q} + \alpha_0$$

with $a_i \in \mathbb{Z}$ for $1 \le i \le d$. We apply Weyl's criterion (Theorem 1.3) with $h = q$ and get

$$\left| \sum_{n=1}^{N} e(q\,f(n)) \right| = \left| \sum_{n=1}^{N} e(q\,\alpha_0) \right| = N.$$

Thus $f(n)$ is not uniformly distributed modulo 1.

Sufficiency: We start by assuming that only α_1 is irrational. Then we write

$$f(x) = \Phi(x) + \alpha_1 x + \alpha_0.$$

Let q be the greatest common divisor of the coefficients of Φ. Obviously $\{\Phi(qx+n)\} = \{\Phi(n)\}$ and we get

$$\begin{aligned}\sum_{n=1}^{N} e(h\,f(n)) &= \sum_{x=1}^{\lfloor \frac{N}{q} \rfloor} \sum_{n=1}^{q} e(h\ (\Phi(n) + \alpha_1(qx+n) + \alpha_0) + \mathcal{O}(q) \\ &= \sum_{n=1}^{q} e\left(h\left(\Phi(n) + \alpha_1 n + \alpha_0\right)\right) \sum_{x=1}^{\lfloor \frac{N}{q} \rfloor} e\left(\left(h\left(\alpha_1 q x\right)\right) + \mathcal{O}(q).\end{aligned}$$

Since α_1 is irrational we get by Lemma 1.5 that

$$\sum_{x=1}^{\lfloor \frac{N}{q} \rfloor} e\left(\left(h\left(\alpha_1 q x\right)\right) = o(N)$$

and thus the sequence is uniformly distributed.

We want to proceed by induction on k, the highest degree term with irrational coefficient. Thus for $k = 1$ we just have shown the theorem. We assume that the theorem holds for k and want to proceed to $k+1$. Then for every positive integer h the highest degree term with irrational coefficient of $f(n+h) - f(n)$ is

$$\alpha_{k+1} h n^k$$

and therefore $(f(n+h) - f(n))_{n\geq 1}$ is uniformly distributed. Now the theorem follows from Theorem 1.7.

□

1.1.2 Discrepancy

When analyzing different uniformly distributed sequences one will realize that there are sequences which are very good distributed, whereas others are far away from an ideal distribution. In order to measure this deviation from the ideal we introduce the discrepancy of a sequence. With help of this we can give a quantitative distinction of uniformly distributed sequences, *i.e.*, we see that some sequences are "good" uniformly distributed and others are rather "bad" uniformly distributed.

Definition 1.8. Let $x_1, \ldots, x_N$ be a finite sequence of real numbers. Then we call

$$D_N(x_1, x_2, \ldots, x_N) := \sup_{0\leq a<b\leq 1} \left| \frac{|\{1 \leq n \leq N : \{x_n\} \in [a,b)\}|}{N} - (b-a) \right|$$

the *discrepancy*.

An obvious consequence of the definition of the discrepancy is the following.

Corollary 1.9. *A sequence $(x_n)_{n\geq 1}$ of real numbers is uniformly distributed if and only if*

$$\lim_{N\to\infty} D_N(x_1, \ldots, x_N) = 0.$$

In order to keep things more simply we define the star discrepancy as follows.

Definition 1.10. For a finite sequence $x_1, \ldots, x_n$ of real numbers, we define

$$D_N^*(x_1, x_2, \ldots, x_N) := \sup_{0<\alpha\leq 1} \left| \frac{|\{1 \leq n \leq N : \{x_n\} \in [0,\alpha)\}|}{N} - \alpha \right|.$$

It is sufficient to consider the star discrepancy, as is shown by the following lemma.

Lemma 1.11 ([47, Theorem 2.1.3])**.**

$$D_N^* \leq D_N \leq 2D_N^*.$$

1.1.3 Generalizations

In chapter 5 we generalize uniform distribution to polynomials finite fields. Therefore let $\mathbb{F}_q[X]$ be the finite field with $q = p^t$ elements. Furthermore let

$$\mathcal{P}_n := \{A \in \mathcal{R} : \deg A < n\}$$

be the set of all polynomials in $\mathbb{F}_q[X]$ whose degree is less than n.

With $\mathbb{F}_q[X]$ and $\mathbb{F}_q(X)$ we have the analogue for the ring of "integers" and the field of "rationals", respectively. To get an equivalent for the "reals" we define a valuation ν as follows. Let $A, B \in \mathbb{F}_q[X]$, then

$$\nu(A/B) := \deg B - \deg A$$

and $\nu(0) := -\infty$. With help of this valuation we can complete $\mathbb{F}_q(X)$ to the field $\overline{\mathbb{F}_q(X)} := \mathbb{F}_q((X^{-1}))$ of formal Laurent series. Then we get

$$\nu\left(\sum_{i=-\infty}^{+\infty} a_i X^i\right) = \sup\{i \in \mathbb{Z} : a_i \neq 0\}.$$

Thus for $A \in \mathbb{F}_q[X]$ we have $\nu(A) = \deg A$.

By the definition of $\overline{\mathbb{F}_q(X)}$ we can write every $\alpha \in \overline{\mathbb{F}_q(X)}$ as

$$\alpha = \sum_{k=-\infty}^{\nu(\alpha)} a_k X^k$$

with $a_k \in \mathbb{F}_q$. Then we call

$$\lfloor\alpha\rfloor := \sum_{k=0}^{\nu(\alpha)} a_k X^k, \quad \{\alpha\} := \sum_{k=-\infty}^{-1} a_k X^k$$

the integral part and the fractional part of α, respectively. The concept of uniform distribution in $\overline{\mathbb{F}_q(X)}$ was first introduced by Carlitz [12]. This was further extended by Dijksma [17, 18] and Car [11].

Definition 1.12. We call a sequence $(\alpha_n)_{n\geq 1}$ of elements in $\overline{\mathbb{F}_q(X)}$ *uniformly distributed* if for every $A \in \mathbb{F}_q(X)$ and every $k \geq 1$ we have

$$\lim_{N\to\infty} \frac{|\{1 \leq n \leq N : \nu(\{\alpha_n - A\}) > k|}{N} = q^k.$$

1.2 Number systems

Before we consider the concept of normal numbers and state our results in this area we have to take a closer look at number systems. These systems together with uniform distribution are essential in the study of normal numbers. We will start with familiar concepts such as the number systems over integers. Let $q < -1$ be a negative integer then every $r \in \mathbb{Z}$ admits a unique and finite representation as follows

$$r = \sum_{k=0}^{\infty} a_k q^k \quad (a_k \in \{0, 1, \dots, |q| - 1\}). \tag{1.2.1}$$

Before we continue we want to explain, what we mean by "unique" and "finite". We call a representation of $r \in \mathbb{Z}$ *unique* if

$$r = \sum_{k=0}^{\infty} a_k q^k = \sum_{k=0}^{\infty} a'_k q^k$$

implies that $a_k = a'_k$ for $k \geq 0$. Furthermore a representation is said to be *finite* if for every $r \in \mathbb{Z}$ there exists an k_0 such that $a_k = 0$ for $k \geq k_0$. This k_0 is called the *length* of the expansion.

Such a representation can be extended to rational numbers and furthermore to real numbers - the completion according to the Euclidean distance. Then every $\alpha \in \mathbb{Q}$ has a representation of the form

$$\alpha = \sum_{k=-\infty}^{\ell} a_k q^k.$$

We define the integer part $\lfloor \alpha \rfloor$ and fractional part $\{\alpha\}$ by

$$\lfloor \alpha \rfloor = \sum_{k=0}^{\ell} a_k q^k, \quad \{\alpha\} = \sum_{k=-\infty}^{-1} a_k q^k.$$

1.2.1 Different number systems

Now we introduce several number systems which will be of interest in the rest of this work.

Matrix number systems

Let $B \in \mathbb{Z}^{n\times n}$ be an expanding matrix (*i.e.*, its eigenvalues have all modulus greater than 1). Let $\mathcal{D} \subset \mathbb{Z}^n$ be a complete set of residues $\pmod B$ with $0 \in \mathcal{D}$. We call the pair $(B, \mathcal{D})$ a (*matrix*) *number system* if every $r \in \mathbb{Z}^n$ admits a representation of the form

$$r = \sum_{k=0}^{\ell-1} B^k a_k, \quad (a_k \in \mathcal{D}).$$

We set $\ell(m) := \ell$ for the *length* of r. As $\mathcal{D}$ is a complete set of residues modulo B, this representation is unique and we furthermore get that $|\mathcal{D}| = [\mathbb{Z}^n : B\mathbb{Z}^n] = |\det B| > 1$.

For $\alpha \in \mathbb{R}^n$ with $\alpha = \sum_{k=-\infty}^{\ell-1} B^k a_k$, we denote by

$$\lfloor \alpha \rfloor := \sum_{k=0}^{\ell-1} B^k a_k, \quad \{\alpha\} := \sum_{k=-\infty}^{-1} B^k a_k,$$

the integral and the fractional part of α, respectively.

Canonical number systems

Let $\mathbb{K}$ be a number field of degree n and $\mathcal{O}_{\mathbb{K}}$ its ring of integers. Fix a $b \in \mathcal{O}_{\mathbb{K}}$ and let $\mathcal{D} := \{0, 1, \ldots, \mathrm{N}(b) - 1\}$, where N denotes the norm over $\mathbb{Q}$. Then we call the pair $(b, \mathcal{D})$ a canonical number system if every $r \in \mathcal{O}_{\mathbb{K}}$ admits a unique finite representation of the form

$$r = \sum_{k=0}^{\ell-1} d_k b^k \quad (d_k \in \mathcal{D}). \tag{1.2.2}$$

We again denote by $\ell(r) := \ell$ the length of the expansion.

Knuth [42] was one of the first considering canonical number systems for the Gaussian integers $\mathbb{Z}[i]$ when he was investigating properties of the "twin-dragon" fractal. These considerations were extended to quadratic number fields by Kátai, Kovács, and Szabó [39, 40, 41]. The extension to the integral domains of algebraic number fields was shown by Kovács and Pethő in [45]. Further extensions to algebraic number fields and matrix number systems are in a series of papers [1, 29, 44, 53, 58].

The connection of matrix number systems and canonical number systems is based on the following observation by Kovács [44]: if b is a base of a canonical number system in a number field then $\{1, b, \dots, b^{n-1}\}$ forms an integral basis for this number field. This implies that there exist canonical number systems in a number field only if this field has a power integral basis. Thus we define an embedding of the following form

$$\begin{array}{cccc} \Phi: & \mathbb{K} & \to & \mathbb{R}^n, \\ & \sum_{k=0}^{n-1} \alpha_k b^k & \mapsto & (\alpha_0, \dots, \alpha_{n-1}). \end{array}$$

Let $m_b(x) = x^n + b_{n-1}x^{n-1} \cdots + b_1 x + b_0$ be the minimal polynomial of b. Then we define the corresponding matrix B to be

$$B := \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 & -b_0 \\ 1 & \ddots & & & \vdots & -b_1 \\ 0 & \ddots & \ddots & & \vdots & -b_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & \ddots & 0 & -b_{n-2} \\ 0 & \cdots & \cdots & 0 & 1 & -b_{n-1} \end{pmatrix}.$$

Then for $\alpha \in \mathbb{K}$

$$\Phi(b\alpha) = B \cdot \Phi(\alpha).$$

This matrix B together with the embedding Φ gives the connection of a canonical number system with its corresponding matrix number system.

Example 1.13 (The Gaussian integers). Let $\mathbb{K} := \mathbb{Z}(i)$ then $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[i]$. As mentioned above one of the first who considered the possible bases was Knuth [42], who was able to show, that $b = -1 \pm i$ is a base. Later this was generalized by Kátai and Szabó [41] who proved that $b = -n \pm i$ with $n \in \mathbb{N}$ is the set of all possible bases for the Gaussian integers.

If we denote by $\overline{b}$ the complex conjugate, then we get that the minimal polynomial of $b = -n \pm i$ is

$$x^2 - (b + \overline{b})\, x + b\overline{b} = x^2 - 2n\, x + (n^2 + 1).$$

Thus we get as matrix B

$$B = \begin{pmatrix} 0 & -(n^2+1) \\ 1 & 2n \end{pmatrix}.$$

Furthermore the relation of matrix number systems to lattice tilings was worked out for instance by Gröchenig and Haas in [29].

Number systems in finite fields

Fix a polynomial $Q \in \mathbb{F}_q[X]$ of positive degree d. It is easy to see that each $A \in \mathbb{F}_q[X]$ admits a unique finite *Q-ary digital expansion*

$$A = \sum_{k=1}^{\ell-1} D_k Q^k \qquad (D_k \in \mathcal{P}_d). \tag{1.2.3}$$

Here we have the property that the length ℓ of the expansion of A is equal to the degree of A plus 1.

Number systems in function fields

Let $p \in \mathbb{F}_q[X, Y]$ be a polynomial. We are now interested in the function field $\mathbb{F}_q(X, Y)/p\mathbb{F}_q(X, Y)$. Number systems in this field have been investigated by Scheicher and Thuswaldner [59] and Beck *et al.* [4].

We write $p(X,Y)$ as a polynomial in $\mathbb{F}_q[X][Y]$, *i.e.*

$$p(X,Y) = p_d Y^d + p_{d-1} Y^{d-1} + \cdots + p_1 Y + p_0.$$

We define the set of digits to be

$$\mathcal{D} := \{A \in \mathbb{F}_q[X] : \deg A < \deg p_0\}.$$

Then we call the pair $(p(X,Y), \mathcal{D})$ a number system if each $Q \in \mathbb{F}_q(X,Y)/p\mathbb{F}_q(X,Y)$ has a unique and finite representation of the form

$$Q = \sum_{k=0}^{\ell-1} D_k Y^k \qquad (D_k \in \mathcal{D}), \tag{1.2.4}$$

We call this representation the Y-ary representation of Q and $L(Q) = \ell$ its length.

For $Q \in \mathbb{F}_q[X]$ and $p(X,Y) = Y - Q$ this corresponds to the definition of Q-ary numbers in $\mathbb{F}_q[X]$ above. By Scheicher and Thuswaldner [59] we get the following characterization.

Proposition 1.14 ([59, Theorem 2.5])**.** *Let $p(X,Y)$ be such that $p_d \in \mathbb{F}_q$ and $\deg p_0 > 0$. Then $(p(X,Y), \mathcal{D})$ is a number system if and only if*

$$\max_{i=1}^{d} \deg p_i < \deg p_0.$$

1.2.2 Fundamental domain

We neglected the fact that the continuation of a number system onto the completion of its field of quotients looses the property of uniqueness. In order to investigate properties such as periodicity and uniqueness of a number system we have to consider the fundamental domain. This domain $\mathcal{F}$ is defined for a matrix number system $(B, \mathcal{D})$ as follows

$$\mathcal{F} = \mathcal{F}(B, \mathcal{D}) := \left\{ \sum_{k \geq 1} B^{-k} d_k : d_k \in \mathcal{D} \right\}.$$

In view of the normal numbers defined below we denote for every $a \in \mathbb{Z}^n$ by

$$\mathcal{F}_a := B^{-\ell(a)}(\mathcal{F} + a)$$

the elements of $\mathcal{F}$ whose $(B, \mathcal{D})$ expansion starts with the same digits as a.

If an $\alpha \in \mathbb{R}^n$ has two or more representation we call it ambiguous, *i.e.*,

$$\alpha = \sum_{k=-\infty}^{\ell} B^k d_k = \sum_{k=-\infty}^{\ell'} B^k d'_k$$

with $d_k \neq d'_k$ for at least one $k \leq \min(\ell, \ell')$. As we will show in chapter 3, these ambiguous representation are in strong connection with the border of the fundamental domain. Moreover we can define the set

$$S := \{q \in \mathbb{Z}^n \setminus \{0\} : \mathcal{F} \cap (\mathcal{F} + q) \neq \emptyset\}.$$

As we will show in chapter 3 this set describes the ambiguous and periodic representations.

For canonical number systems $(b, \mathcal{D})$ the fundamental domain is defined as follows.

$$\mathcal{F} = \mathcal{F}(b, \mathcal{D}) := \left\{ \sum_{k \geq 1} d_k b^{-k} : d_k \in \mathcal{D} \right\}.$$

In the same manner as above for $a \in \mathcal{O}_{\mathbb{K}}$, we denote by

$$\mathcal{F}_a := b^{-\ell(a)}(\mathcal{F} + a)$$

the elements of $\mathcal{F}$ whose b-ary representation starts with the same digits as a.

Example 1.15. We continue the Example 1.13. If we set $b = -1 + i$ then the fundamental domain, which was investigated by Knuth for his “twin-dragon” fractal, looks like Figure 1.1.

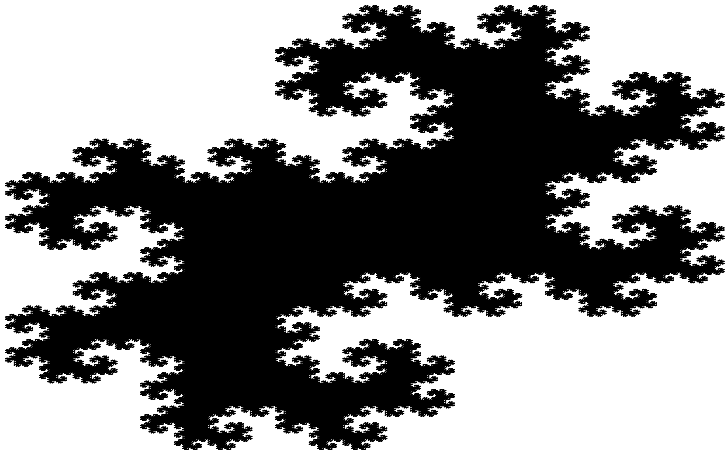

Figure 1.1: $\mathcal{F}(-1+i,\{0,1\})$

1.2.3 Additive functions

Let $q \geq 2$ then we call a function f strictly q-additive if for all positive integers a and all $0 \leq b < q$

$$f(aq+b) = f(a) + f(b)$$

holds. This means that f only acts on the q-ary digits of the argument. A simple example of a strictly q-additive function is the sum of digits function s_q defined for $r \in \mathbb{Z}$ as in (1.2.1)

$$s_q(r) = \sum_{k=0}^{\infty} a_k.$$

In case of number systems for polynomials over a finite field we fix a polynomial $Q \in \mathbb{F}_q[X]$ of degree d. Then we call a function $f : \mathbb{F}_q[X] \to G$ (G some group) strictly Q-additive if it only acts on the digits of the Q-ary representations,*i.e.*, $f(AQ+B) = f(A)+f(B)$ for every $A \in \mathbb{F}_q[X]$ and every $B \in \mathcal{P}_d$. Thus for A with a representation as in (1.2.3) we get

$$f(A) = \sum_{k=0}^{\ell} f(D_k).$$

1.3 Normal numbers

A connection between uniform distribution and digit systems is established by the idea of normal numbers. In an informal way one could say that a number is called normal if every different block of digits occur asymptotically equally often. More formally we let $\theta \in [0,1)$ and $q \geq 2$ be such that

$$\theta = \sum_{k=1}^{\infty} a_k q^{-k}$$

and denote by $\mathcal{N}(\theta; d_1 d_2 d_3 \ldots d_l, N)$ the number of occurrences of the block $d_1 \ldots d_l \in \{0,1,\ldots,q-1\}^l$ in the first n digits, thus

$$\mathcal{N}(\theta; d_1 \ldots d_l, N) := \left|\{0 \leq n < N : a_{n+1} = d_1, \ldots, a_{n+l} = d_l\}\right|.$$

Definition 1.16. We call θ *normal to base* q if for every positive integer l and every block $d_1 \ldots d_l$ of length l

$$\lim_{N\to\infty} \frac{\mathcal{N}(\theta; d_1 \ldots d_l, N)}{N} = q^{-l}.$$

The bridge between normal numbers and uniform distribution is established via the following lemma.

Lemma 1.17 ([47, Theorem 8.1])**.** *The number θ is normal to base b if and only if the sequence $(b^n\theta)_{n\geq 0}$ is uniformly distributed modulo 1.*

Especially the connection between digit systems and their normal numbers give raise to several questions. Most of them are in connection with the properties of the fundamental domain as we will see in the following.

1.3.1 Discrepancy

By considering the relation between uniform distribution and normal numbers established by Lemma 1.17 we could think of carrying over also the idea of the discrepancy to normal numbers. In case of normal numbers the discrepancy describes the deviation from being ideal which in this case considers the block with the biggest difference from equal distribution.

Definition 1.18. Let $\theta \in [0,1)$ and $q \geq 2$. Then the l-discrepancy of θ is defined by

$$\mathcal{R}_{N,l}(\theta) = \sup_{d_1\ldots d_l} \left| \frac{\mathrm{N}(\theta; d_1\ldots d_l, N)}{N} - q^{-l} \right|,$$

where the supremum is over all possible blocks of length l.

The connection of normal numbers and its discrepancy is quite the same as in the uniform distribution case.

Corollary 1.19. *Let $\theta \in [0,1)$ then we call θ normal to base q if and only if for all positive integers l*

$$\lim_{N\to\infty} \mathcal{R}_{N,l} = 0.$$

1.3.2 Generalization

We start by extending the idea of normal numbers to matrix number systems. Let $(B,\mathcal{D})$ be a matrix number system and $\theta \in \mathcal{F}(B,\mathcal{D})$. Then we denote by $\mathcal{N}(\theta; a, N)$ the number of blocks in the first N digits of θ which are equal to the expansion of a. Thus

$$\mathcal{N}(\theta; a, N) := \left|\{0 \leq n < N : \{B^n\theta\} \in \mathcal{F}_a\}\right|.$$

Definition 1.20. We call $\theta \in \mathcal{F}$ *normal in* $(B,\mathcal{D})$ if for every $l \geq 1$ and every $a \in \mathbb{Z}^n$ with $\ell(a) = l$

$$\lim_{N\to\infty} \frac{\mathcal{N}(\theta; a, N)}{N} = |\mathcal{D}|^{-l}. \tag{1.3.1}$$

In view of Definition 1.18 this is equivalent with the following.

Definition 1.21. We call $\theta \in \mathcal{F}$ *normal in* $(B,\mathcal{D})$ if for every $l \geq 1$

$$\sup_{\ell(a)=k} \left| \mathcal{N}(\theta; a, N) - \frac{N}{|\mathcal{D}|^l} \right| = o(N), \tag{1.3.2}$$

where the supremum is taken over all $a \in \mathbb{Z}^n$ whose $(B,\mathcal{D})$ expansion has length l.

Now it is clear what we have to do in order to generalize the idea of normal numbers to canonical number systems. Let $\mathbb{K}$ be a number field of order n and $\mathcal{O}_\mathbb{K}$ its ring of integers. Furthermore let $(b,\mathcal{D})$ be a canonical number system as described above. Then for $\theta \in \mathcal{F}(b,\mathcal{D})$ we define

$\mathrm{N}(\theta; d_1 \dots d_l, N)$ to be the number of occurrences of the block $d_1 \dots d_l \in \mathcal{D}^l$ in the first N digits of θ. If θ has the b-ary representation

$$\theta = \sum_{k \geq 1} a_k b^{-k}$$

and

$$a := \sum_{k=0}^{s-1} r_{s-k} b^k,$$

then $\mathcal{N}$ is defined as

$$\begin{aligned}\mathcal{N}(\theta; r_1 \dots r_s, N) :&= |\{0 \leq n < N : a_{n+1} = d_1, a_{n+2} = d_2, \dots, a_{n+s} = d_s\}| \\ &= |\{0 \leq n < N : \{b^n \theta\} \in \mathcal{F}_a\}| .\end{aligned}$$

Definition 1.22. We call θ *normal in* $(b, \mathcal{D})$ if for every $l \geq 1$

$$\lim_{N \to \infty} \frac{\mathcal{N}(\theta; d_1 \dots d_l, N)}{N} = |\mathcal{D}|^{-l} .$$

This again is equivalent with the following.

Definition 1.23. We call θ *normal in* $(b, \mathcal{D})$ if for every $l \geq 1$ we have that

$$\mathcal{R}_N(\theta) = \mathcal{R}_{N,l}(\theta) := \sup_{d_1 \dots d_l} \left| \frac{1}{N} \mathcal{N}(\theta; d_1 \dots d_l; N) - \frac{1}{|\mathcal{D}|^l} \right| = o(1) \tag{1.3.3}$$

where the supremum is taken over all possible blocks $d_1 \dots d_l \in \mathcal{D}^l$ of length l.

One of our first results in chapter 3 will be the following.

Theorem. *Let $(B, \mathcal{D})$ be a matrix number system. Then every number with an ambiguous representation is not normal.*

By the connection between canonical number systems and matrix number systems it is easy to show the following corollary.

Corollary. *Let $(b, \mathcal{D})$ be a canonical number system. Then every number with an ambiguous representation is not normal.*

1.3.3 Construction

One of the first questions arising from the theory is how many normal numbers are there. The following result is due to E. Borel [6].

Lemma 1.24 ([47, Corollary 8.1])**.** *Almost every number is normal.*

The next is how to construct normal numbers. One idea is to feed a finite automaton with a normal number to construct a different one. These concepts are followed by Dumont, Thomas, and Volkmann in a series of papers [5, 22, 23, 63, 77, 78, 79].

Another way of constructing a normal number is by concatenation of the integer part of functions evaluated at the positive integers. To be more concrete we fix an integer basis $q \geq 2$ and a function f and consider numbers $\theta_q(f)$ of the form

$$\theta_q(f) = 0.\lfloor f(1) \rfloor_q \lfloor f(2) \rfloor_q \lfloor f(3) \rfloor_q \lfloor f(4) \rfloor_q \lfloor f(5) \rfloor_q \lfloor f(6) \rfloor_q \lfloor f(7) \rfloor_q \lfloor f(8) \rfloor_q \lfloor f(9) \rfloor_q \lfloor f(10) \rfloor_q \dots,$$

where $\lfloor \cdots \rfloor_q$ denotes the q-ary integer part.

The simplest construction of this type is due to Champernowne who was able to show that the number

$$0.1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12\,13\,14\,15\,16\,17\,18\ldots$$

is normal to base 10. This equals to $\theta_{10}(f)$ with $f(x) = x$.

This construction has been further generalized by Davenport and Erdős to functions f which have integer values when evaluated on the positive integers. For $f(x)$ a polynomial with *rational* coefficients Schiffer [60] was able to show that $\mathcal{R}_N(\theta_q(f)) = \mathcal{O}(1/\log N)$. In the case of *real* coefficients Nakai and Shiokawa [54] proved the same estimate for $\mathcal{R}_N(\theta_q(f))$.

In his paper Champernowne conjectured that the following number is also normal

$$0.2\,3\,5\,7\,11\,13\,17\,19\,23\,29\,31\,37\,41\,43\ldots$$

to base 10. Copeland and Erdős even proved more. They could show that the number

$$0.a_1\,a_2\,a_3\,a_4\,a_5\,a_6\,a_7\,a_8\,a_9\,a_{10}\,a_{11}\,a_{12}\ldots$$

is normal for every monotonically increasing sequence whose number of elements with $a_i \leq N$ exceeds N^θ for every $\theta < 1$.

In general we again fix an integer basis $q \geq 2$ and a function f and consider constructions of numbers $\tau_q(f)$ of the form

$$\tau_q(f) = 0.\left\lfloor f(2)\right\rfloor_q \left\lfloor f(3)\right\rfloor_q \left\lfloor f(5)\right\rfloor_q \left\lfloor f(7)\right\rfloor_q \left\lfloor f(11)\right\rfloor_q \left\lfloor f(13)\right\rfloor_q \left\lfloor f(17)\right\rfloor_q \left\lfloor f(19)\right\rfloor_q \left\lfloor f(23)\right\rfloor_q \ldots,$$

where the function is evaluated over the primes.

Nakai and Shiokawa [55] showed that $\mathcal{R}_N(\tau_q(f)) = \mathcal{O}(1/\log N)$ for f a function taking integer values when evaluated at the positive integers.

1.3.4 New results

The first new result deals with a further generalization of the result of Nakai and Shiokawa for $\theta_q(f)$ and $\tau_q(f)$. We take f a transcendental entire function of small logarithmic order. An entire function is called transcendental if it is not a polynomial. We say an increasing function $f(r)$ has *logarithmic order* λ if

$$\limsup_{|r|\to\infty} \frac{\log f(r)}{\log\log r} = \lambda < \infty.$$

Then in chapter 2 we show the following two theorems.

Theorem. *Let $f(x)$ be a transcendental entire function which takes real values on the real line. Suppose that the logarithmic order $\alpha = \alpha(f)$ of f satisfies $1 < \alpha < \frac{4}{3}$. Then for any block $d_1 \ldots d_l \in \{0, 1, \ldots, q-1\}^l$, we have*

$$\mathcal{N}(\theta_q(f); d_1 \ldots d_l; N) = \frac{1}{q^l} N + o\left(N\right)$$

as N tends to ∞. The implied constant depends only on f, q, and l.

Theorem. *Let $f(x)$ be a transcendental entire function which takes real values on the real line. Suppose that the logarithmic order $\alpha = \alpha(f)$ of f satisfies $1 < \alpha < \frac{4}{3}$. Then for any block $d_1 \ldots d_l \in \{0, 1, \ldots, q-1\}$, we have*

$$\mathcal{N}(\tau_q(f); d_1 \ldots d_l, N) = \frac{1}{q^l} N + o(N)$$

as N tends to ∞. The implied constant depends only on f, q, and l.

Another topic is the generalization of normal numbers to different number systems. This will be done in chapter 3, where we extend the result of Copeland and Erdős mentioned above to matrix number systems. We yield the following result.

Theorem. *Let $(B, \mathcal{D})$ be a matrix number system and let $\{a_i\}_{i\geq 0}$ be an increasing subsequence of $\{z_i\}_{i\geq 0}$. If for every $\varepsilon > 0$ the number of a_i with $a_i \preceq z_N$ exceeds N^ε for N sufficiently large, then*

$$\theta = 0.[a_0][a_1][a_2][a_3][a_4][a_5][a_6][a_7]\cdots$$

is normal in $(B, \mathcal{D})$ where $[\cdot]$ denotes the expansion in $(B, \mathcal{D})$.

Finally in chapter 4 we generalize the result due to Nakai and Shiokawa for $\theta_q(f)$ to number systems over the Gaussian integers.

Theorem. *Let $f(z) = \alpha_d z^d + \cdots + \alpha_1 z + \alpha_0$ be a polynomial with coefficients in $\mathbb{C}$. Let $(b, \mathcal{D})$ be a canonical number system in the Gaussian integers. Then for every $l \geq 1$*

$$\sup_{d_1\ldots d_l} \left| \frac{1}{N}\mathcal{N}(\theta_b(f); d_1 \ldots d_l; N) - \frac{1}{|\mathcal{D}|^l} \right| = (\log N)^{-1},$$

where the supremum is taken over all blocks of length l.

1.4 Waring's Problem

Despite the applications of exponential sums in uniform distribution there is a very important application in additive number theory. This is connected with the following property.

$$\int_0^1 e(\alpha n)\mathrm{d}\alpha = \begin{cases} 1 & \text{if } n = 0, \\ 0 & \text{else.} \end{cases} \tag{1.4.1}$$

Let s be a positive integer and $\mathcal{S} \subset \mathbb{N}$, then if every $N \in \mathbb{N}$ can be represented as

$$N = x_1 + \cdots + x_s \quad (x_i \in \mathcal{S}) \tag{1.4.2}$$

we call $\mathcal{S}$ a *basis of* $\mathbb{N}$. If this holds only for all $N \geq N_0$ then we call $\mathcal{S}$ an *asymptotic basis* for $\mathbb{N}$. Let $\mathcal{R}(\mathcal{S}, s, N)$ denote the number of solutions of (1.4.2).

If we take $\mathcal{S} := \{n^k : n \in \mathbb{N}\}$ then the above problem is called Waring's Problem. It was first solved for every $k \geq 2$ by Hilbert [34]. Hardy and Littlewood [31, 32] gave a remarkable proof for the asymptotic of $\mathcal{R}(\mathcal{S}, s, N)$ the number of solutions of (1.4.2) for fixed N, s and k. The proof has been further improved and simplified by Vinogradov [72, 69]. He used the following interesting idea motivated by the property in (1.4.1).

$$\begin{aligned} \mathcal{R}(\mathcal{S}, s, N) &= \sum_{\substack{x_1=0\\x_1\in\mathcal{S}}}^{N} \cdots \sum_{\substack{x_s=0\\x_s\in\mathcal{S}}}^{N} \int_0^1 e\left(\alpha(x_1 + \cdots + x_n - N)\right)\mathrm{d}\alpha \\ &= \int_0^1 \left(\sum_{\substack{x=0\\x\in\mathcal{S}}}^{N} e(\alpha\, x) \right)^s e(-\alpha\, N)\mathrm{d}\alpha. \end{aligned}$$

Here we have to consider exponential sums of the form

$$\sum_{\substack{x=0\\x\in\mathcal{S}}}^{N} e(\alpha\, x).$$

The ternary Goldbach problem corresponds to the question if $\mathcal{R}(\mathcal{S}, 3, N)$ is positive for every N and $\mathcal{S} = \{p \in \mathbb{N} : p \text{ prime}\}$. This was solved for sufficiently large N by Vinogradov [73, 70].

For a combination of the Goldbach and Waring's problem, *i.e.*, taking $\mathcal{S} := \{p^k : p \text{ prime}\}$, also asymptotic formulas have been established (*cf.* Hua [37], Vaughan [68]).

1.4.1 Generalizations

Waring's problem has been generalized to number fields, finite fields, polynomials over finite fields, and function fields. The last two will be considered in chapters 5 and 6.

Let $N \in \mathbb{F}_q[X]$, then we call the leading coefficient the *sign* of N, denoted by $\operatorname{sign} N$. Let $\mathcal{P}'_n := \{A \in \mathbb{F}_q[X] : \deg A < n, \operatorname{sign} A = 1\}$ where 1 is the neutral element of the multiplication in $\mathbb{F}_q$.

Let $N \in \mathbb{F}_q[X]$ and $\mathcal{S} \subset \mathbb{F}_q[X]$. We consider an asymptotic formula for the number $\mathcal{R}(\mathcal{S}, s, N)$ of solutions of

$$N = X_1 + \cdots + X_s \quad (X_i \in \mathcal{S}).$$

For $\mathcal{S} = \{A^k : A \in \mathbb{F}_q[X]\}$ an asymptotic formula for $\mathcal{R}(\mathcal{S}, s, N)$ has been independently found by Car [7], Kubota [46] and Webb [82]. This result corresponds to Waring's problem for the polynomials over a finite field. The corresponding ternary Goldbach problem ($\mathcal{S} := \{A \in \mathbb{F}_q[X] : A \text{ irreducible}\}$) has been solved by Hayes [33]. Several other generalizations in the ring $\mathbb{F}_q[X]$ have been considered by Car [8, 11, 9].

1.4.2 Digital restrictions

Above we have defined q-additive functions for a positive integer $q \geq 2$. We fix a $q \geq 2$ and m and h coprime and consider sets of the form

$$\mathcal{S} := \{n^k \in \mathbb{N} : s_q(n) \equiv h \bmod m\}.$$

Thuswaldner and Tichy [65] could give an asymptotic formula for the number of representations $\mathcal{R}(\mathcal{S}, s, N)$.

We want to generalize this result to additive functions in $\mathbb{F}_q[X]$. For $i = 1, \ldots, r$ let f_i denote a Q_i-additive function where $Q_i \in \mathbb{F}_q[X]$ are pairwise coprime polynomials and $d_i := \deg Q_i$. Furthermore let $M_i \in \mathbb{F}_q[X]$ and $m_i = \deg M_i$ for $i = 1, \ldots, r$. Then we define the sets

$$\mathcal{C}_n(\mathbf{f}, \mathbf{J}, \mathbf{M}) = \mathcal{C}_n(\mathbf{J}) := \{A \in \mathcal{P}_n : f_1(A) \equiv J_1 \bmod M_1, \ldots, f_r(A) \equiv J_r \bmod M_r\},$$
$$\mathcal{C}'_n(\mathbf{f}, \mathbf{J}, \mathbf{M}) = \mathcal{C}'_n(\mathbf{J}) := \{A \in \mathcal{P}'_n : f_1(A) \equiv J_1 \bmod M_1, \ldots, f_r(A) \equiv J_r \bmod M_r\}.$$

1.4.3 New results

In chapter 5 we show the uniform distribution of the set $\mathcal{C}_n(\mathbf{f}, \mathbf{J}, \mathbf{M})$.

Theorem. *Let $Q_1, \ldots, Q_r \in \mathbb{F}_q[X]$ be relatively prime and for $i \in \{1, \ldots, r\}$ let f_i be a Q_i-additive function. Choose $M_1, \ldots, M_r, J_1, \ldots, J_r \in \mathbb{F}_q[X]$. Let $\{W_i\}_{i\geq 1}$ be the elements of the set $\mathcal{C}(\mathbf{f}, \mathbf{J}, \mathbf{M})$ defined in (5.2.5) ordered by the relation induced by τ in (5.2.6) and $h(Y) = \alpha_k Y^k + \cdots + \alpha_1 Y + \alpha_0 \in \overline{\mathbb{F}_q(X)}[Y]$ be a polynomial of degree $0 < k < p = \operatorname{char} \mathbb{F}_q$. Then the sequence $h(W_i)$ is uniformly distributed in $\mathcal{K}_\infty$ if and only if at least one coefficient of $h(Y) - h(0)$ is irrational.*

For the corresponding problem of Waring we say that a polynomial $N \in \mathbb{F}_q[X]$ is the *strict* sum of k-th powers if it has a representation of the form

$$N = X_1^k + \cdots + X_s^k \quad (X_1, \ldots, X_s \in \mathcal{C}_n(\mathbf{f}, \mathbf{J}, \mathbf{M})),$$

where the polynomials $X_1, \ldots, X_s$ are each of degree $\leq \lceil \deg N/k \rceil$, *cf.* Definition 1.8 in [24]. Thus the theorem for the strict polynomial Waring reads as follows.

Theorem. *Let $Q_1, \ldots, Q_r \in \mathbb{F}_q[X]$ be relatively prime and for $i \in \{1, \ldots, r\}$ let f_i be a Q_i-additive function. Choose $M_1, \ldots, M_r, J_1, \ldots, J_r \in \mathbb{F}_q[X]$ and set $m_i := \deg M_i$. Suppose that for every $\mathbf{0} \neq \mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}$ there exists an $A \in \mathbb{F}_q[X]$ such that*

$$g_0(A) = E\left(\sum_{i=1}^{r} \frac{R_i}{M_i} f_i(A)\right) \neq 1.$$

Let $N \in \mathbb{F}_q[X]$. If $3 \le k < p = \operatorname{char} \mathbb{F}_q$ and $n \le \lceil \deg N/k \rceil$, then for $s \ge k2^k$ and for every N with sufficiently large $\deg N$ we always get a solution for

$$N = \delta_1 P_1^k + \cdots + \delta_s P_s^k, \quad (P_i \in \mathcal{C}'_n(\mathbf{f}, \mathbf{J}, \mathbf{M}) \text{ for } i = 1, \ldots, s),$$

where $\delta_i \in \mathbb{F}_q$ is a k-th power for $i = 1, \ldots, s$ with $\delta_1 + \cdots + \delta_s = \operatorname{sign} N$.

1.5 Notes

Before we start proving all these new results we want to mention some further literature on the several topics.

Exponential sums. As exponential sums play an important role in different areas of analytic number theory there are several books available. For a good introduction we would recommend the book of Korobov [43].

A deeper insight in the method of exponential pairs, which is important in connection with the estimation of the zero free region of the Riemann zeta-function and the arithmetic estimations of the divisor function, is gained with the book of Graham and Kolesnik [28]. A good basis for Exponential sums, which arise in connection with the Riemann zeta-function, in [67]. Generalizations of exponential sums to multidimensional exponential sums are given in the book of Arkhipov, Chubarikov, and Karatsuba [2].

Uniform distribution and normal numbers. For a general overview on uniform distribution we recommend the book of Kuipers and Niederreiter [47]. An almost complete survey with many references is given by Drmota and Tichy [21].

Number systems. Canonical number systems have been invented by Knuth [42]. A characterization of the possible bases for the Gaussian integers has been given by Kátai and Szabó [41]. These considerations were extended to quadratic number fields by Kátai, Kovács, and Szabó [39, 40, 41]. The extension to the integral domains of algebraic number fields was shown by Kovács and Pethő in [45]. Further extensions to algebraic number fields and matrix number systems are worked out in a series of papers [1, 29, 44, 53, 58].

Matrix number systems have been investigated together with lattice tilings by Gröchenig and Haas in [29].

For number systems in finite fields one may consider Drmota and Gutenbrunner [20].

Properties of the fundamental domains are described in [27, 53, 58, 64].

Waring's Problem. An overview of additive number theory problems such as Waring's Problem, Goldbach's Problem and similar problems is given in Nathanson [56]. For details on Waring's Problem itself one may consider Vaughan [68]. The ternary Goldbach's Problem is considered in Vinogradov [75] and Hua [37]. Finally, exponential sums arising in the problem of Waring-Goldbach are estimated in Hua [37].

Chapter 2

Normality of numbers generated by the values of entire functions

This chapter is based on a joint work with Thuswaldner and Tichy (*cf.* [50]). We want to discuss the case where $f(x)$ is a *transcendental entire function* (i.e., an entire function that is not a polynomial) of small *logarithmic order*. Recall that we say an increasing function $s(r)$ has *logarithmic order* λ if

$$\limsup_{r\to\infty} \frac{\log s(r)}{\log\log r} = \lambda. \tag{2.0.1}$$

we define the *maximum modulus* of an entire function f to be

$$M(r, f) := \max_{|x|\leq r} |f(x)|. \tag{2.0.2}$$

If f is an entire function and $\log M(r, f)$ has logarithmic order λ, then we call f an *entire function of logarithmic order* λ.

To achieve our results we combine the following ingredients.

- The first part of the proofs concerns the estimation for the number of solutions of the equation $f(x) = a$ where $a \in \mathbb{C}$ (cf. [13], [66, Section 8.21]) for entire functions of zero order.
- Following the methods of Nakai and Shiokawa [54, 55] we reformulate the problem in an estimation of exponential sums.
- Finally, the resulting exponential sums are treated by an exponential sum estimate of Baker [3], which was originally used to show that the sequences

  $$(f(n))_{n\geq 1} \qquad \text{and} \qquad (f(p))_{p \text{ prime}}$$

  are uniformly distributed modulo 1 for f an entire function with logarithmic order $1 < \alpha < \frac{4}{3}$.

The main results of this chapter are as follows.

Theorem 2.1. *Let $f(x)$ be a transcendental entire function which takes real values on the real line. Suppose that the logarithmic order $\alpha = \alpha(f)$ of f satisfies $1 < \alpha < \frac{4}{3}$. Then for any block $d_1 \ldots d_l \in \{0, 1, \ldots, q-1\}^l$, we have*

$$\mathcal{N}(\theta_q(f); d_1 \ldots d_l; N) = \frac{1}{q^l} N + o(N)$$

as N tends to ∞. The implied constant depends only on f, q, and l.

For primes we show that $\tau_q(f)$ is normal in the following theorem.

Theorem 2.2. *Let $f(x)$ be a transcendental entire function which takes real values on the real line. Suppose that the logarithmic order $\alpha = \alpha(f)$ of f satisfies $1 < \alpha < \frac{4}{3}$. Then for any block $d_1 \ldots d_l \in \{0, 1, \ldots, q-1\}$, we have*

$$\mathcal{N}(\tau_q(f); d_1 \ldots d_l, N) = \frac{1}{q^l} N + o(N)$$

as N tends to ∞. The implied constant depends only on f, q, and l.

2.1 Notation

Throughout the chapter let f be a transcendental entire function of logarithmic order α satisfying $1 < \alpha < \frac{4}{3}$ and taking real values on the real line. Let

$$f(x) = \sum_{k=1}^{\infty} a_k x^k$$

be the power series expansion of f. By $\log x$ and $\log_q x$ we denote the natural logarithm and the logarithm with respect to base q, respectively. Moreover, we set $e(\beta) := \exp(2\pi i \beta)$.

Let p always denote a prime and $\sum'$ be a sum over primes. By an integer interval I we mean a set of the form $I = \{a, a+1, \ldots, b-1, b\}$ for arbitrary integers a and b.

Furthermore, we denote by $n(r, f)$ the number of zeros of $f(x)$ for $|x| \leq r$.

2.2 Lemmas

First we state the above-mentioned result of Baker that will permit us to estimate exponential sums over entire functions with small logarithmic order by choosing the occurring parameters appropriately.

Lemma 2.3 ([3, Theorem 4])**.** *Let d and h be integers, with $8 \leq h \leq d$. Let $a_1, \ldots, a_d$ be real numbers and suppose that*

$$N^{-h} \exp\left(20 \frac{\log N}{(\log\log N)^2}\right) < |a_h| < \exp(-10^3 h^2), \tag{2.2.1}$$

$$|a_k| \leq \exp\left(-20 \frac{\log N}{(\log\log N)^2}\right) \quad (h < k \leq d). \tag{2.2.2}$$

Suppose further that

$$\log N \geq 10^5 d^3 (\log d)^5. \tag{2.2.3}$$

Then, writing $g(x) = a_d x^d + \cdots + a_1 x$, we have

$$S = \sum_{n \leq N} e(g(n)) \ll N \exp\left(-\frac{1}{2}(\log N)^{\frac{1}{3}}\right) + N \left|a_h\right|^{1/(10h)}. \tag{2.2.4}$$

Lemma 2.4 ([3, Theorem 3])**.** *Under the hypotheses of Lemma 2.3 we have*

$$S = \sum_{p \leq P}{}' e(g(p)) \ll P \exp(-c(\log\log P)^2) + P(\log P)^{-1} \left|a_h\right|^{1/(10h)},$$

where c is a constant depending on g.

The following lemma due to Vinogradov provides an estimate of the Fourier coefficients of certain Urysohn functions.

Lemma 2.5 ([76, Lemma 12]). *Let α, β, Δ be real numbers satisfying*

$$0 < \Delta < \frac{1}{2}, \quad \Delta \leq \beta - \alpha \leq 1 - \Delta.$$

Then there exists a periodic function $\psi(x)$ with period 1, satisfying

1. $\psi(x) = 1$ *in the interval* $\alpha + \frac{1}{2}\Delta \leq x \leq \beta - \frac{1}{2}\Delta$,
2. $\psi(x) = 0$ *in the interval* $\beta + \frac{1}{2}\Delta \leq x \leq 1 + \alpha - \frac{1}{2}\Delta$,
3. $0 \leq \psi(x) \leq 1$ *in the remainder of the interval* $\alpha - \frac{1}{2}\Delta \leq x \leq 1 + \alpha - \frac{1}{2}\Delta$,
4. $\psi(x)$ *has a Fourier series expansion of the form*

$$\psi(x) = \beta - \alpha + \sum_{\substack{\nu=-\infty \\ \nu\neq 0}}^{\infty} A(\nu) e(\nu x),$$

where

$$|A(\nu)| \ll \min\left(\frac{1}{\nu}, \beta - \alpha, \frac{1}{\nu^2\Delta}\right).$$

Finally, we give an easy result on the limit of quotients of sequences that will be used in our proof.

Lemma 2.6. *Let $(a_n)_{n\geq 1}$ and $(b_n)_{n\geq 1}$ be two sequences with $0 < a_n \leq b_n$ for all n and*

$$\lim_{n\to\infty} \frac{a_n}{b_n} = 0. \tag{2.2.5}$$

Then

$$\lim_{n\to\infty} \frac{\sum_{i=1}^n a_i}{\sum_{i=1}^n b_i} = 0.$$

Proof. Let $\varepsilon > 0$ be arbitrary. Then by (2.2.5) there exists an n_0 such that

$$\frac{a_n}{b_n} < \varepsilon/2 \tag{2.2.6}$$

for $n > n_0$. Let $A(N) := \sum_{n=1}^N a_n$ and $B(N) := \sum_{n=1}^N b_n$. We show that there exists a n_1 such that $A(n)/B(n) < \varepsilon$ for $n > n_1$. Therefore we define $C(N) := \sum_{n=n_0+1}^N b_n$. As (2.2.6) implies that $a_n < \frac{\varepsilon}{2} b_n$ for $n > n_0$ we get

$$\frac{A(n)}{B(n)} = \frac{A(n_0) + \sum_{i=n_0+1}^n a_i}{B(n_0) + \sum_{i=n_0+1}^n b_i} < \frac{A(n_0) + \frac{\varepsilon}{2} C(n)}{B(n_0) + C(n)}.$$

As $b_n > 0$ we have that $C(n) \to \infty$ for $n \to \infty$. Thus

$$\lim_{n\to\infty} \frac{A(n_0) + \frac{\varepsilon}{2} C(n)}{B(n_0) + C(n)} = \frac{\varepsilon}{2}.$$

Therefore there is a $n_1 \geq n_0$ such that $A(n)/B(n) \leq \varepsilon$ for $n > n_1$ which proves the lemma. □

2.3 Value Distribution of Entire Functions

Before we start with the proof of the theorems, we need an estimation of the number of solutions for the equation $f(x) = a$ with f a transcendental entire function and $a \in \mathbb{C}$.

In this section we want to show the following result.

Proposition 2.7. *Let f be a transcendental entire function of logarithmic order α. Then for the number of solutions of the equation $f(x) = a$ the following estimate holds.*

$$n(r, f - a) \ll (\log r)^{\alpha - 1}. \tag{2.3.1}$$

As usual in Nevanlinna Theory we do not deal with $n(r, f-a)$ directly but use a strongly related function, which is defined by

$$N(r, f) = \int_1^r \frac{n(t, f) - n(0, f)}{t} dt - n(0, f) \log r \tag{2.3.2}$$

in order to prove the proposition. The connection between $n(r, f-a)$ and $N(r, f-a)$ is illustrated in the following lemma.

Lemma 2.8 ([13, Theorem 4.1])**.** *Let $f(x)$ be a non-constant meromorphic function in $\mathbb{C}$. For each $a \in \mathbb{C}$, $N(r, f-a)$ is of logarithmic order $\lambda+1$, where λ is the logarithmic order of $n(r, f-a)$.*

The next lemma provides us with a very good estimation of the order of $N(r, f - a)$.

Lemma 2.9 ([57, Theorem])**.** *If f is an entire function of logarithmic order α where $1 < \alpha \leq 2$, then for all values $a \in \mathbb{C}$*

$$\log M(r, f) \sim N(r, f - a) \sim \log M\left(r(\log r)^{2-\alpha}\right) \sim N\left(r(\log r)^{2-\alpha}\right).$$

Now it is easy to prove Proposition 2.7.

Proof of Proposition 2.7. As f fulfils the assumptions of Lemma 2.9 we have that

$$N(r, f - a) \sim M(r, f) \ll (\log r)^{\alpha}. \tag{2.3.3}$$

Thus we have that $N(r, f-a)$ is of logarithmic order α and therefore by Lemma 2.8 we get that $n(r, f - a)$ is of logarithmic order $\alpha - 1$. □

2.4 Proof of Theorem 2.1

We fix the block $d_1 \dots d_l$ throughout the proof. Moreover, we adopt the following notation. Let $\mathcal{N}(f(n))$ be the number of occurrences of the block $d_1 \dots d_l$ in the q-ary expansion of the integer part $\lfloor f(n) \rfloor$. Furthermore, denote by $\ell(m)$ the length of the q-ary expansion of the integer m, i.e., $\ell(m) = \lfloor \log_q m \rfloor + 1$. Define M by

$$\sum_{n=1}^{M-1} \ell(f(n)) < N \leq \sum_{n=1}^{M} \ell(f(n)). \tag{2.4.1}$$

Because f is of logarithmic order $\alpha < \frac{4}{3}$ we easily see that

$$\ell(f(n)) \ll (\log M)^{\alpha} \qquad (1 \leq n \leq M).$$

Thus

$$\left| \mathcal{N}(\theta_q(f); d_1 \dots d_l; N) - \sum_{n=1}^{M} \mathcal{N}(f(n)) \right| \ll lM$$

We denote by J and $\bar{J}$ the maximum length and the average length of $\lfloor f(n) \rfloor$ for $n \in \{1, \ldots, N\}$, respectively, i.e.,

$$\begin{aligned} J &:= \max_{1 \le n \le M} \ell(\lfloor f(n) \rfloor) \ll\gg (\log M)^\alpha, \\ \bar{J} &:= \frac{1}{M} \sum_{n=1}^{M} \ell(\lfloor f(n) \rfloor) \ll\gg (\log M)^\alpha, \end{aligned} \tag{2.4.2}$$

where $\ll\gg$ stands for both $\ll$ and $\gg$. Note that from these definitions we immediately see that

$$N = M\bar{J} + \mathcal{O}((\log M)^\alpha). \tag{2.4.3}$$

Thus in order to prove the theorem it suffices to show

$$\sum_{n=1}^{M} \mathcal{N}(f(n)) = \frac{1}{q^l} N + o\left(N\right). \tag{2.4.4}$$

In order to count the occurrences of the block $d_1 \ldots d_l$ in the q-ary expansion of $\lfloor f(n) \rfloor$ ($1 \le n \le M$) we define the indicator function

$$\mathcal{I}(t) = \begin{cases} 1 & \text{if } \sum_{i=1}^{l} d_i q^{-i} \le t - \lfloor t \rfloor < \sum_{i=1}^{l} d_i q^{-i} + q^{-l}, \\ 0 & \text{otherwise} \end{cases} \tag{2.4.5}$$

which is an 1-periodic function. Indeed, write $f(n)$ in q-ary expansion for every $n \in \{1, \ldots, M\}$, i.e.,

$$f(n) = b_r q^r + b_{r-1} q^{r-1} + \ldots b_1 q + b_0 + b_{-1} q^{-1} + \ldots,$$

then the function $\mathcal{I}(t)$ is defined in a way that

$$\mathcal{I}(q^{-j} f(n)) = 1 \Longleftrightarrow d_1 \ldots d_l = b_{j-1} \ldots b_{j-l}.$$

In order to write $\sum_{n \le M} \mathcal{N}(f(n))$ properly in terms of $\mathcal{I}$ we define the subsets $I_l, \ldots, I_J$ of $\{1, \ldots, M\}$ by

$$n \in I_j \Leftrightarrow f(n) \ge q^j \qquad (l \le j \le J).$$

Every I_j consists of those $n \in \{1, \ldots, M\}$ for which we can shift the q-ary expansion of $\lfloor f(n) \rfloor$ at least j digits to the right to count the occurrences of the block $d_1 \ldots d_l$. Using these sets we get

$$\sum_{n \le M} \mathcal{N}(f(n)) = \sum_{j=l}^{J} \sum_{n \in I_j} \mathcal{I}\left(\frac{f(n)}{q^j}\right). \tag{2.4.6}$$

In the next step we fix j and show that $I_j = I_j(M)$ consists of integer intervals which are of asymptotically increasing length for M increasing. As I_j consists of all n such that $f(n) \ge q^j$ these n have to be between two zeros of the equation $f(x) = q^j$. By Proposition 2.7 the number of solutions for this equation is $n(M, f - q^j) \ll (\log M)^{\alpha-1}$. Therefore we can split I_j into k_j integer subintervals

$$I_j = \bigcup_{i=1}^{k_j} \{n_{ji}, \ldots, n_{ji} + m_{ji} - 1\}$$

where m_{ji} is the length of the integer interval and $k_j \ll (\log M)^{\alpha-1}$. Thus the length of the integer intervals is increasing, i.e., $M(\log M)^{1-\alpha} \ll m_{ji} \ll M$. Thus we get that

$$\sum_{n \le M} \mathcal{N}(f(n)) = \sum_{j=l}^{J} \sum_{i=1}^{k_j} \sum_{n_{ji} \le n < n_{ji} + m_{ji}} \mathcal{I}\left(\frac{f(n)}{q^j}\right). \tag{2.4.7}$$

Following Nakai and Shiokawa [54, 55] we want to approximate $\mathcal{I}$ from above and from below by two 1-periodic functions having small Fourier coefficients. In particular, we set

$$\begin{aligned} \alpha_- &= \sum_{\lambda=1}^{l} d_\lambda q^{-\lambda} + (2\delta_i)^{-1}, \quad \beta_- = \sum_{\lambda=1}^{l} d_\lambda q^{-\lambda} + q^{-l} - (2\delta_i)^{-1}, \quad \Delta_- = \delta_i^{-1}, \\ \alpha_+ &= \sum_{\lambda=1}^{l} d_\lambda q^{-\lambda} - (2\delta_i)^{-1}, \quad \beta_+ = \sum_{\lambda=1}^{l} d_\lambda q^{-\lambda} + q^{-l} + (2\delta_i)^{-1}, \quad \Delta_+ = \delta_i^{-1}. \end{aligned} \tag{2.4.8}$$

We apply Lemma 2.5 with $(\alpha,\beta,\Delta) = (\alpha_-,\beta_-,\Delta_-)$ and $(\alpha,\beta,\Delta) = (\alpha_+,\beta_+,\Delta_+)$, respectively, in order to get two functions $\mathcal{I}_-$ and $\mathcal{I}_+$. By the choices of $(\alpha_\pm,\beta_\pm,\Delta_\pm)$ it is immediate that

$$\mathcal{I}_-(t) \le \mathcal{I}(t) \le \mathcal{I}_+(t) \qquad (t \in \mathbb{R}). \tag{2.4.9}$$

Lemma 2.5 also implies that these two functions have Fourier expansions

$$\mathcal{I}_\pm(t) = q^{-l} \pm \delta_i^{-1} + \sum_{\substack{\nu=-\infty \\ \nu\neq 0}}^{\infty} A_\pm(\nu) e(\nu t) \tag{2.4.10}$$

satisfying

$$|A_\pm(\nu)| \ll \min(|\nu|^{-1}, \delta_i |\nu|^{-2}). \tag{2.4.11}$$

In a next step we want to replace $\mathcal{I}$ by $\mathcal{I}_+$ in (2.4.6). To this matter we observe, using (2.4.9), that

$$|\mathcal{I}(t) - \mathcal{I}_+(t)| \le |\mathcal{I}_+(t) - \mathcal{I}_-(t)| \ll \delta_i^{-1} + \sum_{\substack{\nu=-\infty \\ \nu\neq 0}}^{\infty} A_\pm(\nu) e(\nu t).$$

Together with (2.4.6) this implies that

$$\sum_{n\le M} \mathcal{N}(f(n)) = \sum_{j=l}^{J} \sum_{i=1}^{k_j} \sum_{n_{ji}\le n < n_{ji}+m_{ji}} \left(\mathcal{I}_+\left(\frac{f(n)}{q^j}\right) + \mathcal{O}\left(\delta_i^{-1} + \sum_{\substack{\nu=-\infty \\ \nu\neq 0}}^{\infty} A_\pm(\nu) e\left(\nu \frac{f(n)}{q^j}\right)\right)\right).$$

Inserting the Fourier expansion of $\mathcal{I}_+$ this yields

$$\sum_{n\le M} \mathcal{N}(f(n)) = \sum_{j=l}^{J} \sum_{i=1}^{k_j} \sum_{n_{ji}\le n < n_{ji}+m_{ji}} \left(\frac{1}{q^l} + \mathcal{O}\left(\delta_i^{-1} + \sum_{\substack{\nu=-\infty \\ \nu\neq 0}}^{\infty} A_\pm(\nu) e\left(\nu \frac{f(n)}{q^j}\right)\right)\right). \tag{2.4.12}$$

Because of the definition of M and $\bar{J}$ in (2.4.1) and (2.4.2), respectively, and the estimate in (2.4.3) we get that

$$\sum_{j=l}^{J} \sum_{i=1}^{k_j} \sum_{n_{ji}\le n < n_{ji}+m_{ji}} 1 = \bar{J}M + \mathcal{O}(lM) = N + \mathcal{O}(lM). \tag{2.4.13}$$

Inserting this in (2.4.12) and subtracting the main part Nq^{-l} we obtain

$$\left| \sum_{n\le M} \mathcal{N}(f(n)) - \frac{N}{q^l} \right| \ll \sum_{j=l}^{J} \sum_{i=1}^{k_j} \sum_{n_{ji}\le n < n_{ji}+m_{ji}} \left(\delta_i^{-1} + \sum_{\substack{\nu=-\infty \\ \nu\neq 0}}^{\infty} A_\pm(\nu) e\left(\frac{\nu}{q^j} f(n)\right)\right) + lM. \tag{2.4.14}$$

Now we consider the coefficients $A_\pm(\nu)$. Noting (2.4.11) one sees that

$$A_\pm(\nu) \ll \begin{cases} \nu^{-1} & \text{for } |\nu| \le \delta_i, \\ \delta_i \nu^{-2} & \text{for } |\nu| > \delta_i. \end{cases}$$

Estimating trivially all summands with $|\nu| > \delta$ we get

$$\sum_{\substack{\nu=-\infty \\ \nu\neq 0}}^{\infty} A_\pm(\nu) e\left(\frac{\nu}{q^j} f(n)\right) \ll \sum_{\nu=1}^{\delta_i} \nu^{-1} e\left(\frac{\nu}{q^j} f(n)\right) + \delta_i^{-1}. \tag{2.4.15}$$

Using this in (2.4.14) and changing the order of summation yields

$$\left|\sum_{n\le M} \mathcal{N}(f(n)) - \frac{N}{q^l}\right| \ll \sum_{j=l}^{J} \sum_{i=1}^{k_j} \sum_{n_{ji}\le n < n_{ji}+m_{ji}} \left(\delta_i^{-1} + \sum_{\nu=1}^{\delta_i} \nu^{-1} e\left(\frac{\nu}{q^j} f(n)\right)\right) + lM. \tag{2.4.16}$$

The crucial part is now to estimate the exponential sum containing the entire function f. Define

$$S(X) := \sum_{n\le X} e\left(\frac{\nu}{q^j} f(n)\right). \tag{2.4.17}$$

We now treat the sum $S(X)$ by a similar reasoning as in the proof of Baker [3, Theorem 2]. We will show that the sum only depends on f and X.

To this matter we let the parameter d occurring in Lemma 2.3 be a function of X, in particular, we set

$$d = d(X) = \lfloor 10^{-2} (\log X)^{1/3} (\log\log X)^{-2} \rfloor, \tag{2.4.18}$$

which tends to infinity with X (see equation (11) of [3]). Moreover, we define the polynomial

$$g_j(x) = \frac{\nu}{q^j}(a_1 x + \cdots + a_d x^d)$$

by the first d summands of the power series of $\frac{\nu}{q^j} f$. The parameter h of Lemma 2.3 will also be a function of X. In particular, we set $h = h(X)$ to be the largest positive integer such that $h \le d$ and

$$X^{-h+\frac{1}{2}} < \left|\frac{\nu}{q^j} a_h\right|. \tag{2.4.19}$$

As shown in [3], h also tends to infinity with X.

Up to now we have not chosen a value for δ_i. For the moment, we just assume that $\delta_i \le h$ because this choice implies that the summation index ν varies only over positive integers that are less than h. Thus the logarithmic order of $\frac{\nu}{q^j} f(n)$ is less than $\frac{4}{3}$. Indeed,

$$\log\left(\frac{\nu}{q^j} f(n)\right) < \log h - j\log q + \log f(n) < \log\log X + (\log X)^\alpha < (\log X)^{\bar\alpha} \tag{2.4.20}$$

where $\bar\alpha = \alpha + \varepsilon < \frac{4}{3}$. Note that g_j satisfies the conditions of Lemma 2.3. The estimate for the logarithmic order of $\frac{\nu}{q^j} f(n)$ will enable us to replace f by g_j in (2.4.17) causing only a small error term. This will then permit us to apply Lemma 2.3 in order to estimate $S(X)$.

By (2.4.20), equation (15) of [3] implies that for d as in (2.4.18)

$$\sum_{t>d} \left|\frac{\nu}{q^j} a_t\right| X^t < (2X)^{-1} \tag{2.4.21}$$

and therefore (see [3])

$$\left|\sum_{n\leq X} e\left(\frac{\nu}{q^j} f(n)\right)\right| \leq \left|\sum_{n\leq X} e(g_j(n))\right| + \pi.$$

By this we can use Baker's estimations for exponential sums over entire functions contained in Lemma 2.3 and get with $d = d(X)$ and $h = h(X)$ defined in (2.4.18) and (2.4.19), respectively,

$$S(X) \ll X \exp(-\tfrac{1}{2}(\log X)^{\frac{1}{3}}) + X \exp(-h). \tag{2.4.22}$$

Now it is time to set δ_i for every i. As ν changes the coefficients of the function under consideration we calculate for every $\nu = 1, \ldots, d(m_{ji})$ the corresponding $h_\nu(m_{ji})$. In order to fulfil the constraint on the logarithmic order we need to chose δ_i smaller than the smallest $h_\nu(m_{ji})$ with $\nu \leq \delta_i$. Thus we set

$$\delta_i := \max\{r \leq d(m_{ji}) : r \leq \min\{h_\nu(m_{ji}) : \nu \leq r\}\}. \tag{2.4.23}$$

This is always possible since $h_\nu(m_{ji}) \geq 1$. For this choice we also have $\delta_i \leq h_\nu(m_{ji})$ and $\delta_i \to \infty$ as $m_{ji} \to \infty$ because the minimum of the $h_\nu(m_{ji})$ tends to infinity for $m_{ji} \to \infty$. Doing this for every $i = 1, \ldots, k$ (i.e., for every integer interval comprising the set I_j) we can apply (2.4.22) with $X = m_{ji}$ and use the fact that δ_i is the smallest $h_\nu(m_{ji})$ for i. This yields

$$\begin{aligned}\sum_{i=1}^{k_j}\sum_{\nu=1}^{\delta_i} \nu^{-1} \sum_{n_{ji}\leq n<n_{ji}+m_{ji}} e\left(\frac{\nu}{q^j} f(n)\right) &\ll \sum_{i=1}^{k_j}\sum_{\nu=1}^{\delta_i} \nu^{-1} S(m_{ji}) \\ &\ll \sum_{i=1}^{k_j}\sum_{\nu=1}^{\delta_i} \nu^{-1} m_{ji} \exp(-\tfrac{1}{2}(\log m_{ji})^{\frac{1}{3}}) + m_{ji}\exp(-\delta_i) \\ &\ll \sum_{i=1}^{k_j} \Big(m_{ji} \exp(-\tfrac{1}{2}(\log m_{ji})^{\frac{1}{3}}) + m_{ji}\exp(-\delta_i)\Big) \log \delta_i.\end{aligned}$$

As we do not know the asymptotic behavior of δ_i we have to distinguish the cases whether $\exp(-\delta_i)$ is greater or smaller than $\exp(-\frac{1}{2}(\log m_{ji})^{\frac{1}{3}})$. In both cases we can assume that m_{ji} is sufficiently large.

- Suppose first that $\exp(-\frac{1}{2}(\log m_{ji})^{\frac{1}{3}}) > \exp(-\delta_i)$ holds. As $\delta_i \leq d(m_{ji}) \leq (\log m_{ji})^{1/3}$ we get

  $$\exp(-\tfrac{1}{2}(\log m_{ji})^{\frac{1}{3}}) \log \delta_i \ll \exp(-\tfrac{1}{2}(\log m_{ji})^{\frac{1}{3}})(\log\log m_{ji}) \ll \exp(-\tfrac{1}{3}(\log m_{ji})^{\frac{1}{3}})$$

  and thus

  $$\Big(\exp(-\tfrac{1}{2}(\log m_{ji})^{\frac{1}{3}}) + \exp(-\delta_i)\Big) \log \delta_i \ll \exp(-\tfrac{1}{3}(\log m_{ji})^{\frac{1}{3}}) + \exp(-\delta_i/2).$$

- For the second case assume that $\exp(-\frac{1}{2}(\log m_{ji})^{\frac{1}{3}}) \leq \exp(-\delta_i)$ holds. This implies that $\log \delta_i \ll \log\log m_{ji}$ and we get

  $$\exp(-\tfrac{1}{2}(\log m_{ji})^{\frac{1}{3}}) \log \delta_i \ll \exp(-\tfrac{1}{2}(\log m_{ji})^{\frac{1}{3}})(\log\log m_{ji}) \ll \exp(-\tfrac{1}{3}(\log m_{ji})^{\frac{1}{3}}).$$

  Therefore we also have

  $$\Big(\exp(-\tfrac{1}{2}(\log m_{ji})^{\frac{1}{3}}) + \exp(-\delta_i)\Big) \log \delta_i \ll \exp(-\tfrac{1}{3}(\log m_{ji})^{\frac{1}{3}}) + \exp(-\delta_i/2).$$

By this we have the estimation

$$\sum_{\nu=1}^{\delta_i}\nu^{-1}\sum_{n_{ji}\leq n<n_{ji}+m_{ji}} e\left(\frac{\nu}{q^j}f(n)\right)\ll\sum_{i=1}^{k}m_{ji}\left(\exp(-\tfrac{1}{3}(\log m_{ji})^{\frac{1}{3}})+\exp(-\delta_i/2)\right). \tag{2.4.24}$$

By (2.4.16) we get that

$$\left|\sum_{n\leq M}\mathcal{N}(f(n))-\frac{N}{q^l}\right|\ll\sum_{j=l}^{J}\sum_{i=1}^{k_j}\sum_{n_{ji}\leq n<n_{ji}+m_{ji}}\left(\delta_i^{-1}+\sum_{\nu=1}^{\delta}\nu^{-1}e\left(\frac{\nu}{q^j}f(n)\right)\right)+lM$$

Thus it remains to show that

$$\sum_{i=1}^{k_j}\sum_{n_{ji}\leq n<n_{ji}+m_{ji}}\delta^{-1}=\sum_{i=1}^{k_j}\frac{m_{ji}}{\delta_i}=o(|I_j|). \tag{2.4.25}$$

and

$$\sum_{i=1}^{k_j}\sum_{n_{ji}\leq n<n_{ji}+m_{ji}}\sum_{\nu=1}^{\delta_i}\nu^{-1}e\left(\frac{\nu}{q^j}f(n)\right)=o\left(|I_j|\right), \tag{2.4.26}$$

where $|I_j|=\sum_{i=1}^{k_j}m_{ji}$ the sum of the lengths of the integer intervals.

First we consider (2.4.25). Therefore we set $a_i=\frac{m_{ji}}{\delta_i}$ and $b_i=m_{ji}$. By noting that $\frac{a_i}{b_i}=\delta_i^{-1}\to 0$ we are able to apply Lemma 2.6 and get

$$0\leq\frac{\sum_{i=1}^{k}\frac{m_{ji}}{\delta_i}}{\sum_{i=1}^{k}m_{ji}}\to 0.$$

Finally we have to show (2.4.26). We again want to apply Lemma 2.6 by setting

$$\begin{aligned}a_i &:= m_{ji}\exp(-\tfrac{1}{3}(\log m_{ji})^{\frac{1}{3}})+m_{ji}\exp(-\delta_i/2),\\ b_i &:= m_{ji}.\end{aligned}$$

As $M(\log M)^{1-\alpha}\ll m_{ji}\ll M$ we get that both $\exp(-\frac{1}{3}(\log m_{ji})^{\frac{1}{3}})$ and $\exp(-\delta_i/2)$ tend to zero. Thus we have that $\frac{a_i}{b_i}\to 0$ for $M\to\infty$. An application of Lemma 2.6 together with (2.4.24) gives

$$0\leq\frac{\sum_{\nu=1}^{\delta}\nu^{-1}\sum_{n_{ji}\leq n<n_{ji}+m_{ji}}e\left(\frac{\nu}{q^j}f(n)\right)}{|I_j|}\ll\frac{\sum_{i=1}^{k}m_{ji}\left(\exp(-\frac{1}{3}(\log m_{ji})^{\frac{1}{3}})+\exp(-\delta_i/2)\right)}{\sum_{i=1}^{k}m_{ji}}\to 0$$

for $M\to\infty$ and thus (2.4.26) holds.

We put (2.4.25) and (2.4.26) in our estimate (2.4.16) and get together with (2.4.13) that

$$\begin{aligned}\left|\sum_{n\leq M}\mathcal{N}(f(n))-\frac{N}{q^l}\right| &\ll\sum_{j=l}^{J}\sum_{i=1}^{k_j}\sum_{n_{ji}\leq n<n_{ji}+m_{ji}}\left(\delta_i^{-1}+\sum_{\nu=1}^{\delta}\nu^{-1}e\left(\frac{\nu}{q^j}f(n)\right)\right)+lM\\ &\ll\sum_{j=l}^{J}o(|I_j|)+lM=o(\bar{J}M)=o(N).\end{aligned}$$

Thus by (2.4.4) the theorem is proven.

2.5 Proof of Theorem 2.2

Throughout the proof p will always denote a prime and $\pi(x)$ will denote the number of primes less than or equal to x. As in the proof of Theorem 2.1 we fix the block $d_1 \dots d_l$ and write $\mathcal{N}(f(p))$ for the number of occurrences of this block in the q-ary expansion of $\lfloor f(p) \rfloor$. By $\ell(m)$ we denote the length of the q-ary expansion of an integer m. We define an integer P by

$$\sum_{p \leq P-1}{}' \ell\left(\lfloor f(p) \rfloor\right) < N \leq \sum_{p \leq P}{}' \ell\left(\lfloor f(p) \rfloor\right). \tag{2.5.1}$$

As above we get that

$$\ell(\lfloor f(p) \rfloor) \leq (\log P)^{\alpha} \quad (2 \leq p \leq P).$$

Again we set J the greatest and $\bar{J}$ the average length of the q-ary expansions over the primes. Thus

$$J := \max_{p \leq P \text{ prime}} \ell(\lfloor f(p) \rfloor) \ll\gg (\log P)^{\alpha} \tag{2.5.2}$$

$$\bar{J} := \frac{1}{\pi(P)} \sum_{p \leq P}{}' \ell(\lfloor f(p) \rfloor) \ll\gg (\log P)^{\alpha}. \tag{2.5.3}$$

Note that by these definitions we have

$$N = \bar{J}P + \mathcal{O}((\log P)^{\alpha}). \tag{2.5.4}$$

Thus by the same reasoning as in the proof of Theorem 2.1 it suffices to show that

$$\sum_{p \leq P}{}' \mathcal{N}(f(p)) = \frac{N}{q^l} + o(N). \tag{2.5.5}$$

We define the indicator function as in (2.4.5) and also the subsets $I_l, \dots, I_J$ of $\{2, \dots, P\}$ by

$$n \in I_j \Leftrightarrow f(n) \geq q^j \qquad (l \leq j \leq J).$$

Following the proof of Theorem 2.1 we see that

$$\sum_{p \leq P}{}' \mathcal{N}(f(p)) = \sum_{j=l}^{J} \sum_{p \in I_j}{}' \mathcal{I}\left(\frac{f(p)}{q^j}\right) + \mathcal{O}\left(l\pi(P)\right). \tag{2.5.6}$$

Now we fix j and split I_j into k_j integer intervals of length m_{ji} for $i = 1, \dots, k$. Thus

$$I_j = \bigcup_{i=1}^{k_j} \{n_{ji}, n_{ji}+1, \dots, n_{ji}+m_{ji}-1\}$$

By Proposition 2.7 we again get that $k_j \ll (\log P)^{\alpha-1}$. Thus the length of the m_{ji} is asymptotically increasing for P, indeed, we have $P(\log P)^{1-\alpha} \ll m_{ji} \ll P$. Now we can rewrite (2.5.6) by

$$\sum_{p \leq P}{}' \mathcal{N}(f(p)) = \sum_{j=l}^{J} \sum_{i=1}^{k_j} \sum_{n_{ji} \leq p < n_{ji}+m_{ji}}{}' \mathcal{I}\left(\frac{f(p)}{q^j}\right) + \mathcal{O}\left(l\pi(P)\right). \tag{2.5.7}$$

Following Nakai and Shiokawa [54, 55] again we get as in the proof of Theorem 2.1 that there exist two functions $\mathcal{I}_-$ and $\mathcal{I}_+$. We replace $\mathcal{I}$ by $\mathcal{I}_+$ in (2.5.7) and together with the Fourier expansion of $\mathcal{I}_+$ in (2.4.10) we get in the same manner as in (2.4.12) that

$$\sum_{p \leq P}{}' \mathcal{N}(f(p)) = \sum_{j=l}^{J} \sum_{i=1}^{k_j} \sum_{n_{ji} \leq p < n_{ji}+m_{ji}}{}' \left(\frac{1}{q^j} + \mathcal{O}\left(\delta_i^{-1} + \sum_{\substack{\nu=-\infty \\ \nu \neq 0}}^{\infty} A_{\pm}(\nu) e\left(\nu \frac{f(n)}{q^j}\right)\right)\right). \tag{2.5.8}$$

By (2.5.1) and (2.5.2) together with (2.5.4) we have

$$\sum_{j=l}^{J}\sum_{i=1}^{k_j}\sum_{n_{ji}\le p<n_{ji}+m_{ji}}{}' 1 = \bar{J}\pi(P)+\mathcal{O}(l\pi(P)) = N+\mathcal{O}(l\pi(P)). \tag{2.5.9}$$

We subtract the main part Nq^{-l} in (2.5.8) and get by (2.5.9)

$$\left|\sum_{p\le P}{}'\mathcal{N}(f(p))-\frac{N}{q^l}\right| \ll \sum_{j=l}^{J}\sum_{i=1}^{k_j}\sum_{n_{ji}\le p<n_{ji}+m_{ji}}{}'\left(\delta_i^{-1}+\sum_{\substack{\nu=-\infty\\ \nu\neq 0}}^{\infty}A_{\pm}(\nu)e\left(\frac{\nu}{q^j}f(n)\right)\right)+l\pi(P). \tag{2.5.10}$$

We estimate the coefficients $A_{\pm}(\nu)$ in the same way as in (2.4.15). Then (2.5.10) simplifies to

$$\left|\sum_{p\le P}{}'\mathcal{N}(f(p))-\frac{N}{q^l}\right| \ll \sum_{j=l}^{J}\sum_{i=1}^{k_j}\sum_{n_{ji}\le p<n_{ji}+m_{ji}}{}'\left(\delta_i^{-1}+\sum_{\nu=1}^{\delta_i}\nu^{-1}e\left(\frac{\nu}{q^j}f(p)\right)\right)+l\pi(P). \tag{2.5.11}$$

Again the crucial part is the estimation of an exponential sum over the primes. We apply quite the same reasoning as in the proof of Theorem 2.1. We set

$$S'(X) := \sum_{p\le X}{}' e\left(\frac{\nu}{q^j}f(p)\right). \tag{2.5.12}$$

and use the functions $d(X)$ and $h(X)$ defined in (2.4.18) and (2.4.19), respectively. If we assume that $\delta_i \le h(X)$ then we get that the logarithmic order of $\frac{\nu}{q^j}f(x)$ is less than $\frac{4}{3}$ as in (2.4.20). We set

$$g_j(x) = \frac{\nu}{q^j}(a_d x^d + \cdots + a_1 x).$$

By (2.4.21) we also get that

$$\left|\sum_{p\le X}{}' e\left(\frac{\nu}{q^j}f(p)\right)\right| \le \left|\sum_{p\le X}{}' e\left(g_j(p)\right)\right| + \pi.$$

We can apply Lemma 2.4 to get the estimate

$$S'(X) \ll X\exp(-c_\nu(\log\log X)^2)+\frac{X}{\log X}\exp(-h), \tag{2.5.13}$$

where c_ν is a constant depending on ν and $h = h(X)$ is the function defined in (2.4.19).

Now we fix i and for every $\nu = 1,\dots,d(m_{ji})$ we calculate the corresponding $h_\nu(m_{ji})$ and c_ν. We set

$$\delta_i := \max\{r \le d(m_{ji}) : r \le \min\{h_\nu(m_{ji}) : \nu \le r\}\}, \tag{2.5.14}$$
$$\bar{c}_i := \min\{c_\nu : \nu = 1,\dots,\delta_i\}.$$

By the above reasoning we have that $\delta_i \to \infty$ for m_{ji} and therefore for P.

By this we get a δ_i for every $i = 1,\dots,k$ and we can estimate the exponential sum in (2.5.11) with help of (2.5.13) and the definitions of δ_i and $\bar{c}_i$ in (2.5.14) to get

$$\begin{aligned}\sum_{i=1}^{k_j}\sum_{n_{ji}\le p<n_{ji}+m_{ji}}{}'\sum_{\nu=1}^{\delta_i}\nu^{-1}e\left(\frac{\nu}{q^j}f(p)\right) &\ll \sum_{i=1}^{k_j}\sum_{\nu=1}^{\delta_i}\nu^{-1}S'(m_{ji})\\ &\ll \sum_{i=1}^{k_j}\sum_{\nu=1}^{\delta_i}\nu^{-1}m_{ji}\left(\exp(-\bar{c}_i(\log\log m_{ji})^2)+\frac{\exp(-\delta_i)}{\log m_{ji}}\right)\\ &\ll \sum_{i=1}^{k_j}m_{ji}\left(\exp(-\bar{c}_i(\log\log m_{ji})^2)+\frac{\exp(-\delta_i)}{\log m_{ji}}\right)\log\delta_i.\end{aligned} \tag{2.5.15}$$

As we do not know the asymptotic behavior of δ_i we want to merge it with the expression in the parenthesis and therefore have to distinguish two cases according whether $\exp(-\delta_i)(\log m_{ji})^{-1}$ is greater or smaller than $\exp(-\bar{c}_i(\log\log m_{ji})^2)$.

- If $\exp(-\bar{c}_i(\log\log m_{ji})^2) > \exp(-\delta_i)(\log m_{ji})^{-1}$ then as $\delta_i \leq (\log P)^{1/3}$ we have that

$$\exp(-\bar{c}_i(\log\log m_{ji})^2)\log\delta_i \leq \exp(-\bar{c}_i(\log\log m_{ji})^2)\log\log m_{ji} < \exp(-\bar{c}_i/2(\log\log m_{ji})^2).$$

  Thus

$$\begin{aligned}\big(\exp(-\bar{c}_i(\log\log m_{ji})^2) + \exp(-\delta_i)(\log m_{ji})^{-1}\big)\log\delta_i \\ \ll \exp(-\bar{c}_i/2(\log\log m_{ji})^2) + \exp(-\delta_i/2)(\log m_{ji})^{-1}.\end{aligned}$$

- On the contrary we have $\exp(-\bar{c}_i(\log\log m_{ji})^2) \leq \exp(-\delta_i)(\log m_{ji})^{-1}$ and this implies $\delta_i \leq c(\log\log m_{ji})^2$ for a positive constant c. Therefore we get

$$\exp(-\bar{c}_i(\log\log m_{ji})^2)\log\delta_i \leq \exp(-\bar{c}_i(\log\log m_{ji})^2)c(\log\log m_{ji})^2 < \exp(-\bar{c}_i/2(\log\log m_{ji})^2).$$

  We again have

$$\begin{aligned}\big(\exp(-\bar{c}_i(\log\log m_{ji})^2) + \exp(-\delta_i)(\log m_{ji})^{-1}\big)\log\delta_i \\ \ll \exp(-\bar{c}_i/2(\log\log m_{ji})^2) + \exp(-\delta_i/2)(\log m_{ji})^{-1}.\end{aligned}$$

By this we have

$$\begin{aligned}\sum_{i=1}^{k_j}\sum_{\nu=1}^{\delta_i}\nu^{-1}\sideset{}{'}\sum_{n_{ji}\leq p<n_{ji}+m_{ji}} e\left(\frac{\nu}{q^j}f(p)\right) \\ \ll \sum_{i=1}^{k_j} m_{ji}\left(\exp(-\bar{c}_i/2(\log\log m_{ji})^2) + \exp(-\delta_i/2)(\log m_{ji})^{-1}\right). \quad (2.5.16)\end{aligned}$$

The considerations above can be used in (2.5.11) in order to obtain

$$\left|\sideset{}{'}\sum_{p\leq P}\mathcal{N}(f(p)) - \frac{N}{q^l}\right| \ll \sum_{j=l}^{J}\sum_{i=1}^{k_j}\sideset{}{'}\sum_{n_{ji}\leq p<n_{ji}+m_{ji}}\left(\delta_i^{-1} + \sum_{\nu=1}^{\delta_i}\nu^{-1}e\left(\frac{\nu}{q^j}f(p)\right)\right) + l\pi(P).$$

Thus it remains to show that

$$\sum_{i=1}^{k_j}\sideset{}{'}\sum_{n_i\leq p<n_i+m_{ji}}\delta_i^{-1} = o(\pi(I_j)) \quad (2.5.17)$$

and

$$\sum_{\nu=1}^{\delta_i}\nu^{-1}\sum_{i=1}^{k_j}\sideset{}{'}\sum_{n_{ji}\leq p<n_{ji}+m_{ji}} e\left(\frac{\nu}{q^j}f(p)\right) = o(\pi(I_j)), \quad (2.5.18)$$

where $\pi(I_j)$ stands for the number of primes in the interval I_j.

First we have to estimate the number of primes in I_j for every j. Therefore we set $m'_{ji} := \pi(\{n_{ji},\ldots,n_{ji}+m_{ji}-1\})$. Thus the number of primes in I_j is the sum of the m'_{ji}, i.e. $\pi(I_j) = \sum_{i=1}^{k_j} m'_{ji}$. As

$$P(\log P)^{1-\alpha} \ll m_{ji} \ll P \quad (i = 1,\ldots,k_j) \quad (2.5.19)$$

holds we consider an integer interval $[x-y,x]\cap\mathbb{Z}$ with $x(\log x)^{1-\alpha}\leq y<x$. We set $y:=x\beta^{-1}$ and get

$$1<\beta\leq(\log x)^{\alpha-1}. \tag{2.5.20}$$

To estimate the number of primes we apply the Prime Number Theorem in the following form (which is a weaker result than in Chapter 11 of [16]).

$$\pi(x)=\frac{x}{\log x}+\mathcal{O}\left(\frac{x}{(\log x)^2}\right). \tag{2.5.21}$$

Thus we get with (2.5.20) and (2.5.21)

$$\begin{aligned}\pi\left([x-y,x]\cap\mathbb{Z}\right)&=\pi(x)-\pi(x-y)\\&=\frac{x}{\log x}-\frac{x-x\beta^{-1}}{\log(x-x\beta^{-1})}+\mathcal{O}\left(\frac{x}{(\log x)^2}\right)\\&=\frac{x}{\log x}-\frac{x-x\beta^{-1}}{\log x+\mathcal{O}\left(\beta^{-1}\right)}+\mathcal{O}\left(\frac{x}{(\log x)^2}\right)\\&=\frac{x}{\log x}-\frac{x-x\beta^{-1}}{\log x}(1+\mathcal{O}\left(\beta^{-1}(\log x)^{-1}\right))+\mathcal{O}\left(\frac{x}{(\log x)^2}\right)\\&=\frac{y}{\log x}+\mathcal{O}\left(\frac{x}{(\log x)^2}\right).\end{aligned} \tag{2.5.22}$$

Now we reformulate (2.5.22) by setting $x=P$ and $y=m_{ji}$ and get with (2.5.19)

$$m_{ji}'=\pi\left(\{n_i,\dots,n_i+m_{ji}-1\}\right)=\frac{m_{ji}}{\log P}+\mathcal{O}\left(\frac{P}{(\log P)^2}\right). \tag{2.5.23}$$

Now we use the estimation (2.5.23) in order to show (2.5.17). By setting $a_i=\frac{m_{ji}'}{\delta_i}$ and $b_i=m_{ji}'$ we note that as $m_{ji}'\to\infty$ we get that $m_{ji}\to\infty$ which implies $\frac{a_i}{b_i}\to 0$. Therefore we can apply Lemma 2.6 and get

$$0\leq\frac{\sum'_{p\in I_j}\delta^{-1}}{\pi(I_j)}=\frac{\sum_{i=1}^k\frac{m_{ji}}{\delta_i}}{\sum_{i=1}^k m_{ji}'}\to 0.$$

Finally we show that (2.5.18) holds. We set

$$\begin{aligned}a_i&=m_{ji}(\exp(-\bar{c}_i/2(\log\log m_{ji})^2)+\exp(-\delta_i/2)(\log m_{ji})^{-1}),\\b_i&=m_{ji}'.\end{aligned}$$

By the estimation in (2.5.23) we get that $\frac{a_i}{b_i}\to 0$ for $P\to\infty$ and we are able to apply Lemma 2.6. Thus with (2.5.16) we get

$$\begin{aligned}0\leq\frac{\sum_{i=1}^{k_j}\sum_{\nu=1}^{\delta}\nu^{-1}\sum'_{n_{ji}\leq p<n_{ji}+m_{ji}}e\left(\frac{\nu}{q^j}f(p)\right)}{\pi(I_j)}\\ \ll\frac{\sum_{i=1}^{k_j}m_{ji}(\exp(-\bar{c}_i/2(\log\log m_{ji})^2)+\exp(-\delta_i/2)(\log m_{ji})^{-1})}{\sum_{i=1}^{k_j}m_{ji}'}\to 0.\end{aligned}$$

Thus by putting (2.5.11), (2.5.18), and (2.5.17) together we get

$$\begin{aligned}\left|\sum_{p\leq P}{}'\mathcal{N}(f(p))-\frac{N}{q^l}\right|&\ll\sum_{j=l}^{J}\sum_{i=1}^{k_j}\sum_{n_{ji}\leq p<n_{ji}+m_{ji}}{}'\left(\delta_i^{-1}+\sum_{\nu=1}^{\delta_i}\nu^{-1}e\left(\frac{\nu}{q^j}f(p)\right)\right)+l\pi(P)\\&\ll\sum_{j=l}^{J}o(\pi(I_j))+l\pi(P)\ll o(\bar{J}P)\ll o(N),\end{aligned}$$

which, together with (2.5.5), proves Theorem 2.2.

Chapter 3

Normal numbers in matrix number systems

This chapter is based on a work of Madritsch [51]. We want to generalize the result of Copeland and Erdős to matrix number systems. Therefore we fix a matrix number system $(b, \mathcal{D})$.

For our generalization it is not necessary that $(B, \mathcal{D})$ is a number system. We are interested in a wider class of pairs $(B, \mathcal{D})$, which Indlekofer,*et.al.* [38] call *just touching covering systems* (JTCS). A pair $(B, \mathcal{D})$ is a JTCS if

$$\lambda((m_1 + \mathcal{F}) \cap (m_2 + \mathcal{F})) = 0, \quad (m_1 \neq m_2, \quad m_1, m_2 \in \mathbb{Z}^n)$$

where λ denotes the n-dimensional Lebesgue measure.

As the representation of an element is not necessarily unique in a JTCS, we have to define and to consider ambiguous expansions. Later we will show that an element with an ambiguous expansion cannot be normal.

3.1 Numbering the elements of a JTCS

To show the structure of elements of $(B, \mathcal{D})$ we mainly follow [53]. First we define the map

$$\begin{aligned} \Phi : \mathbb{Z}^n &\to \mathbb{Z}^n \\ x &\mapsto B^{-1}(x - a) \end{aligned}$$

where $a \in \mathcal{D}$ is the representative of the congruence class of x (*i.e.*, $x - a \in B\mathbb{Z}^n$).

We define $\mathcal{P} := \left\{ m \in \mathbb{Z}^n : \exists k \in \mathbb{N} : \Phi^k(m) = m \right\}$ to be the set of *periodic* elements, which is finite (*cf.* [53]). Now we construct a unique representation of every $m \in \mathbb{Z}^n$. Therefore let $r = r(m) \geq 0$ be the least integer such that $\Phi^r(m) = p \in \mathcal{P}$. Then every $m \in \mathbb{Z}^n$ has a unique representation as follows:

$$m = \sum_{j=0}^{r-1} B^j a_j + B^r p \quad (a_j \in \mathcal{D}, p \in \mathcal{P})$$

with $\Phi^{r-1}(m) = a_{r-1} + Bp \notin \mathcal{P}$ if $r \geq 1$.

We denote by

$$\mathcal{R} := \left\{ \sum_{j=0}^{k} B^j a_j : k \geq 0, a_j \in \mathcal{D} \right\}$$

the set of all *properly representable* elements of $\mathbb{Z}^n$.

We want to define an ordering on this set. Therefore let $q := |\det B|$ and let τ be a bijection from $\mathcal{D}$ to $\{0, \dots, q-1\}$ such that $\tau(0) = 0$. Then we extend τ on $\mathcal{R}$ by setting $\tau(a_k B^k + \cdots + a_1 B + a_0) := \tau(a_k)q^k + \cdots + \tau(a_1)q + \tau(a_0)$. We also pull back the relation $\leq$ from $\mathbb{N}$ to $\mathcal{R}$ by setting

$$a \preceq b :\Leftrightarrow \tau(a) \leq \tau(b), \quad (a, b \in \mathcal{R}). \tag{3.1.1}$$

Then we define a sequence $\{z_i\}_{i\geq 0}$ of elements in $\mathcal{R}$ with $z_i := \tau^{-1}(i)$. This sequence is increasing, *i.e.*, $i \leq j \Rightarrow \ell(z_i) \leq \ell(z_j)$ and $z_i \preceq z_j$ for $i, j \in \mathbb{N}$.

Now we can state our main results.

Theorem 3.1. *Let $(B, \mathcal{D})$ be a JTCS and let $\{a_i\}_{i\geq 0}$ be an increasing subsequence of $\{z_i\}_{i\geq 0}$. If for every $\varepsilon > 0$ the number of a_i with $a_i \preceq z_N$ exceeds N^ε for N sufficiently large, then*

$$\theta = 0.[a_0][a_1][a_2][a_3][a_4][a_5][a_6][a_7]\cdots$$

is normal in $(B, \mathcal{D})$ where $[\cdot]$ denotes the expansion in $(B, \mathcal{D})$.

Before we state the proof of the theorem we have to exclude the case that θ is ambiguous (*i.e.*, has two different representations). In the next section we will show that any $\theta \in \mathcal{F}$ with two different representations cannot be normal.

3.2 Ambiguous expansions in JTCS

We call a $\theta \in \mathcal{F}$ *ambiguous* (with ambiguous expansion) if there exists a $l \geq 0$ such that

$$\{B^l \theta\} \in \partial\mathcal{F}. \tag{3.2.1}$$

In the following lines we will justify our definition. If a $\theta \in \mathcal{F}$ has two different expansions this means that there exist $l \geq 1$ and $a_i, b_i \in \mathcal{D}$ for $i = 1, 2, \dots$ with

$$\theta = \sum_{i=1}^{\infty} B^{-i} a_i = \sum_{i=1}^{\infty} B^{-i} b_i \quad \text{and} \quad a_l \neq b_l.$$

This equals saying that there exist an $m \in \mathbb{Z}^n$ and a $l \geq 0$ such that

$$\{B^l \theta\} \in \mathcal{F} \cap (m + \mathcal{F}).$$

We set

$$S := \{m \in \mathbb{Z}^n \setminus \{0\} : \mathcal{F} \cap (m + \mathcal{F}) \neq \emptyset\}, \quad S_0 := S \cup \{0\}, \quad B_m := \mathcal{F} \cap (m + \mathcal{F}).$$

By Lemma 3.1 of [53] we see that

$$\partial\mathcal{F} = \bigcup_{m\in S} B_m.$$

Thus all $\theta \in \mathcal{F}$, which satisfy (3.2.1), have at least two different expansions.

Since l is finite and we are interested in the asymptotical distribution of blocks in the digital expansion and since $B^l\mathcal{F} \cap \mathcal{F} = \mathcal{F}$ we may assume without loss of generality that $l = 0$.

The goal of this section is to show the following Theorem.

Theorem 3.2. *If $\theta \in \mathcal{F}$ is ambiguous, then θ is not normal.*

We follow [53] to construct the graph $G(\mathbb{Z}^n)$, which provides a tool for constructing the representation of an element of S_0. For this graph $\mathbb{Z}^n$ is its set of vertices and $\mathcal{B} := \mathcal{D} - \mathcal{D}$ its set of labels. The rule for drawing an edge is the following

$$m_1 \xrightarrow{b} m_2 :\Longleftrightarrow Bm_1 - m_2 = b \in \mathcal{B} \quad (m_1, m_2 \in \mathbb{Z}^n).$$

By $G(S)$ and $G(S_0)$ we define the restrictions of $G(\mathbb{Z}^n)$ to the sets S and S_0, respectively.

By Remark 3.4 of [53] we get that any infinite walk $m \xrightarrow{b_1} m_2 \xrightarrow{b_2} m_3 \xrightarrow{b_3} \cdots$ in $G(S_0)$ yields a representation

$$m = \sum_{j\geq 1} B^{-j} b_j.$$

Vice versa by looking at such a representation of m we get an infinite walk in $G(S_0)$, starting at m.

Now we construct the graph $\overline{G}(S_0)$ to determine all points of B_m. Therefore we define for every pair (m_1, m_2)

$$\mathcal{C}(m_1, m_2) := \{a \in \mathcal{D} : (Bm_1 + \mathcal{D}) \cap (m_2 + a) \neq \emptyset\} \quad \text{and} \quad c_{m_1,m_2} := |\mathcal{C}(m_1, m_2)|.$$

Now the graph $\overline{G}(S_0)$ results from $G(S_0)$ by replacing every edge $m_1 \xrightarrow{b} m_2$ by c_{m_1,m_2} edges $m_1 \xrightarrow{a} m_2$ with $a \in \mathcal{C}(m_1, m_2)$. By the considerations in Remark 3.4 of [53] we furthermore get that every infinite walk $m \xrightarrow{a_1} m_2 \xrightarrow{a_2} m_3 \xrightarrow{a_3} \cdots$ in $\overline{G}(S_0)$ yields a point

$$\theta = \sum_{j\geq 1} B^{-j} a_j \in B_m \subset \partial\mathcal{F}.$$

We denote by $C := (c_{k,l})_{k,l\in S}$ the accompanying matrix of $\overline{G}(S)$ and call it the *contact matrix* (*cf.*, (6) of [29]). Similarly we call $\overline{G}(S)$ the *contact graph* of $(B, \mathcal{D})$.

Thus every ambiguous point $\theta \in \mathcal{F}$ can be constructed by an infinite walk in $\overline{G}(S_0)$. If we can show that there exists a sufficiently long walk which could not be constructed by $\overline{G}(S_0)$, then we get that the corresponding block does not appear in any ambiguous point and hence the ambiguous points cannot be normal.

Therefore we denote by $W_k(m)$ the set of all different walks of length k starting at m in $\overline{G}(S_0)$. Further let W_k be the total set of walks of length k in $\overline{G}(S_0)$. Then we simply get

$$|W_k| = \sum_{m\in S} |W_k(m)|.$$

By the definition of the contact matrix C and noting that $(|W_0(m)|)_{m\in S} = (1, \ldots, 1)^t$ we get the recurrence

$$(|W_{k+1}(m)|)_{m\in S} = C \cdot (|W_k(m)|)_{m\in S}.$$

Let $\mu_{\max}$ be the eigenvalue of largest modulus of C. Then there exists a constant $c > 0$ such that

$$|W_k| = \sum_{m\in S} |W_k(m)| = c\mu_{\max}^k (1 + o(1)). \tag{3.2.2}$$

Thus we are left with an estimation of $\mu_{\max}$. Therefore we justify our naming of C and use the following result.

Lemma 3.3 ([29, Theorem 2.1]). *If $(B, \mathcal{D})$ is a JTCS, then*

$$|\mu_{max}| < |\det B|.$$

Now the proof of Theorem 3.2 follows easily.

Proof of Theorem 3.2. In order to show that an ambiguous number θ is not normal we need to show that there exists a block of length k that cannot occur in the $(B, \mathcal{D})$-expansion of θ.

By the considerations above this is equivalent to showing that there exists a block of length k that cannot occur as a labeling of a walk of length k in $\overline{G}(S)$.

Since the number of possible blocks of length k is $|\mathcal{D}|^k$ and the number of walks of length k is $|W_k|$ it suffices to show

$$|W_k| \leq |\mathcal{D}|^k - 1.$$

Thus putting (3.2.2) and Lemma 3.3 together we get that there exists a $k_0 > 0$ such that

$$|W_k| = c\mu_{\max}^k (1 + o(1)) \leq |\det B|^k - 1 = |\mathcal{D}|^k - 1 \quad (k \geq k_0).$$

□

3.3 Proof of Theorem 3.1

The proof works in three steps.

1. We start by using the ordering function τ to transfer the number to a number in q-ary expansion for $q := |\det B|$.
2. Then we apply the Theorem of Copeland and Erdős to show the normality of this transfered number.
3. Finally transferring the number back to a JTCS we show that this does not affect normality.

First we transpose the problem in the setting of q-ary expansions where $q := |\det B| > 1$. Therefore we use our numbering function τ to transfer θ into a q-ary expansion. Thus

$$\tau(\theta) := 0.[\tau(a_0)][\tau(a_1)][\tau(a_2)][\tau(a_3)][\tau(a_4)][\tau(a_5)][\tau(a_6)][\tau(a_7)]\cdots,$$

where $[\cdot]$ denotes the q-ary expansion. As it will always be clear we use $[\cdot]$ for the $(B,\mathcal{D})$- and the q-ary expansion simultaneously.

By the assumptions of the theorem we get that $\{\tau(a_i)\}_{i\geq 0}$ is an increasing sequence and we can apply the Theorem of Copeland and Erdős.

Lemma 3.4 ([15, Theorem])**.** *If $a_1, a_2, \ldots$ is an increasing sequence of integers such that for every $\varepsilon < 1$ the number of a's up to N exceeds N^ε provided N is sufficiently large, then the infinite decimal*

$$0.a_1a_2a_3a_4a_5a_6\ldots$$

is normal with respect to the base q in which these integers are expressed.

Applying Lemma 3.4 gives that $\tau(\theta)$ is normal. Thus for $k \geq 1$, $M \geq k$ and $(d_1, \ldots, d_k) \in \{0, 1, \ldots, q-1\}^k$

$$\left|\left\{k \leq n \leq M+k \middle| \exists\, a \in \mathbb{Z} : \lfloor q^n\tau(\theta)\rfloor = aq^k + \sum_{i=0}^{k-1} d_iq^i\right\}\right| = \frac{M}{q^k} + o(M). \tag{3.3.1}$$

For an $x \in \mathbb{Z}$ with

$$x = \sum_{i=0}^{k} a_iq^i,$$

where $0 \leq a_i < q$ for every i, we define $\ell(x) := k+1$ to be the q-ary length of x. Then it is clear that $\ell(a) = \ell(\tau(a))$ for all $a \in \mathcal{R}$.

For $k \geq 1$ and $a \in \mathcal{R}$ with $\ell(a) = k$ we get together with (3.3.1) that

$$\begin{aligned}\mathcal{N}(\theta; a, N) &= |\{0 \leq n < N | \{B^n\theta\} \in \mathcal{F}_a\}| \\ &= \left|\left\{k \leq n \leq N+k \middle| \exists\, a \in \mathbb{Z} : \lfloor q^n\tau(\theta)\rfloor = aq^k + \tau(a)\right\}\right| \\ &= \frac{N}{q^k} + o(N) = \frac{N}{|\mathcal{D}|^k} + o(N).\end{aligned}$$

By noting the definition of normality in (1.3.2) the theorem is proven.

Chapter 4

Generating normal numbers over Gaussian integers

In this chapter we consider a construction of normal numbers which is due to Madritsch [52]. Since we want to construct a normal number as a concatenation of digital expansions of a certain sequence of numbers we have to give an ordering for the Gaussian integers which will fit our purpose. Therefore we set $q := N(b)$ where N denotes the Norm of b over $\mathbb{Q}$ and let τ be a bijection between $\mathcal{D}$ and $\{0, 1, \ldots, q-1\}$ with $\tau(0) = 0$. Then we extend τ to the Gaussian integers by setting $\tau(d_0 + d_1 b + d_2 b^2 + \cdots + d_k b^k) := \tau(d_0) + \tau(d_1)q + \tau(d_2)q^2 + \cdots + \tau(d_k)q^k$. Furthermore we pull back the relation $\leq$ from $\mathbb{N}$ to $\mathbb{Z}[i]$ by

$$a \leq b :\Leftrightarrow \tau(a) \leq \tau(b), \quad a, b \in \mathbb{Z}[i].$$

By this we define a sequence $\{z_n\}_{n\geq 1}$ of elements of $\mathbb{Z}[i]$ such that $z_n := \tau^{-1}(n-1)$.

For a function $f : \mathbb{Z}[i] \to \mathbb{C}$ we define

$$\theta_b(f) := \theta(f) = \lfloor f(z_1) \rfloor q^{-\ell(f(z_1))} + \lfloor f(z_2) \rfloor q^{-\ell(f(z_1))-\ell(f(z_2))} + \cdots .$$

This is simply the concatenation of the integer parts of the function values evaluated on the sequence $\{z_n\}_{n\geq 1}$ of Gaussian integers. We are now in a position to state our main theorem.

Theorem 4.1. *Let $f(z) = \alpha_d z^d + \cdots + \alpha_1 z + \alpha_0$ be a polynomial with coefficients in $\mathbb{C}$. Let $(b, \mathcal{D})$ be a CNS in the Gaussian integers. Then for every $l \geq 1$*

$$\sup_{d_1 \ldots d_l} \left| \frac{1}{N} \mathcal{N}(\theta_b(f); d_1 \ldots d_l; N) - \frac{1}{|\mathcal{D}|^l} \right| = (\log N)^{-1},$$

where the supremum is taken over all blocks of length l.

4.1 Preliminary Lemmata

As we deal with blocks of a certain length we need information about the connection of the norm of a Gaussian integer and the length of its expansion. This connection is described by the following lemma.

Lemma 4.2 ([27, Proposition 2.6]). *Let $(b, \mathcal{D})$ be a number system in the Gaussian integers and $q := N(b)$. Then the estimate*

$$\left| \ell(z) - \log_q |z|^2 \right| \leq c_b,$$

where $\log_q$ is the logarithm in base q, holds for a certain constant c_b depending only on the base b.

In the proof of our main result we will need the discrepancy (see [21, p.5] for a definition) $D_N(\boldsymbol{x}_n)$ of the first N elements of a sequence $\{\boldsymbol{x}_n\}_{n\geq 1}$ of elements in $\mathbb{R}^2$. The following result will provide us with an estimation of the discrepancy.

Lemma 4.3 (Erdös-Turan-Koksma inequality, [21, Theorem 1.21]). *Let $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N$ be points in $\mathbb{R}^2$ and T an arbitrary positive integer. Then*

$$D_N(\boldsymbol{x}_n) \leq \left(\frac{3}{2}\right)^k \left(\frac{2}{V+1} + \sum_{0<\|\boldsymbol{v}\|_\infty \leq V} \frac{1}{r(\boldsymbol{v})} \left|\frac{1}{N}\sum_{n=1}^{N} e(\boldsymbol{v}\cdot\boldsymbol{x}_n)\right|\right),$$

where $r(\boldsymbol{v}) = (\max\{1, |v_1|\}) \cdot (\max\{1, |v_2|\})$ for $\boldsymbol{v} = (v_1, v_2) \in \mathbb{Z}^2$.

For the transformation of an exponential sum into an integral we will apply the two following lemmata.

Lemma 4.4 ([2, Lemma 5.4]). *Suppose that $F(x_1, \ldots, x_r)$ is a real differentiable function for $0 \leq x_j \leq P_j$, $P_j \leq P$ $(j = 1, \ldots, r)$, inside the interval of variation of the variables, the function $\partial F(x_1, \ldots, x_r)/\partial x_j$ is piecewise monotone and of constant sign in each of the variables x_j $(j = 1, \ldots, r)$ for any fixed values of the other variables, and the number of intervals of monotonicity and constant sign does not exceed s. Next, let the inequalities*

$$\left|\frac{\partial F(x_1, \ldots, x_r)}{\partial x_j}\right| \leq \delta, \quad j = 1, \ldots, r,$$

hold for $0 < \delta < 1$. Then

$$\sum_{x_1=0}^{P_1} \cdots \sum_{x_r=0}^{P_r} e(F(x_1, \ldots, x_r))$$
$$= \int_0^{P_1} \cdots \int_0^{P_r} e(F(x_1, \ldots, x_r))\mathrm{d}x_1 \ldots \mathrm{d}x_r + \theta_1 rsP^{r-1}\left(3 + \frac{2\delta}{1-\delta}\right),$$

where $|\theta_1| \leq 1$.

Lemma 4.5 ([67, Lemma 4.2]). *Let $F(x)$ be a real differentiable function such that $F'(x)$ is monotonic, and $F'(x) \geq m > 0$, or $F'(x) \leq -m < 0$, throughout the interval $[a, b]$. Then*

$$\left|\int_a^b e(F(x))\mathrm{d}x\right| \leq \frac{4}{m}.$$

In the next lemma we give an application of the preceding ones.

Lemma 4.6. *Let M and N be positive integers with $M \ll N$. Let $F : \mathbb{C} \to \mathbb{C}$ be a function such that the conditions of Lemma 4.4 and Lemma 4.5 are fulfilled. Then*

$$\sum_{M\leq|z|^2<M+N} e(\operatorname{tr} F(z)) \ll \frac{\sqrt{N}}{m} + \frac{N}{(\log N)^{\sigma/2}} + s\left(\frac{3-\delta}{1-\delta}\right)\sqrt{N(\log N)^\sigma}$$

holds for any positive real number σ. Here $\operatorname{tr}(x)$ denotes the trace of an element $x \in \mathbb{Z}[i]$.

Proof. This is a generalization of [26, Lemma 2.1 and 2.2]. In order to apply the two lemmas above we start considering squares in the annulus $M \leq |z|^2 < M + N$. Therefore we denote by $D_\nu := \{z = x + iy \in \mathbb{Z}[i] : -\nu \leq x, y \leq \nu\}$. Now we get by an application of Lemma 4.4 that

$$\sum_{z\in D_\nu} e(\operatorname{tr} F(z)) = \sum_{x=-\nu}^{\nu}\sum_{y=-\nu}^{\nu} e(\operatorname{tr} F(x+iy))$$

$$= \int_{-\nu}^{\nu}\int_{-\nu}^{\nu} e(\operatorname{tr} F(x+iy))\mathrm{d}x\mathrm{d}y + 2\theta_1 s\nu\left(\frac{3-\delta}{1-\delta}\right)$$

We take the modulus in order to apply Lemma 4.5. Thus

$$\begin{aligned}\left|\sum_{z\in D_\nu} e(\operatorname{tr} F(z))\right| &\leq \int_{-\nu}^{\nu}\left|\int_{-\nu}^{\nu} e(\operatorname{tr} F(x+iy))\mathrm{d}x\right|\mathrm{d}y + 2\theta_1 s\nu\left(\frac{3-\delta}{1-\delta}\right)\\ &\leq 2\nu \max_{-\nu\leq y\leq\nu}\left|\int_{-\nu}^{\nu} e(\operatorname{tr} F(x+iy))\mathrm{d}x\right| + 2\theta_1 s\nu\left(\frac{3-\delta}{1-\delta}\right)\\ &\leq \frac{8\nu}{m} + 2\theta_1 s\nu\left(\frac{3-\delta}{1-\delta}\right)\end{aligned}$$

Secondly we tessellate the annulus $M \leq |z|^2 < M+N$ by squares of side length $\sqrt{N/(\log N)^\sigma}$. We define two sets I and B containing the squares which are completely inside the annulus and those which intersect the boundary, respectively. Then we denote by C_I and C_B their contribution to the sum, respectively. There are $\mathcal{O}((\log N)^\sigma)$ squares in I and together with our considerations above we get that

$$C_I \ll \frac{N}{m} + s\left(\frac{3-\delta}{1-\delta}\right)\sqrt{N(\log N)^\sigma}.$$

For C_B we get that we can cover the boundary by two annuls of width $\mathcal{O}(\sqrt{M/(\log M)^\sigma})$ and $\mathcal{O}(\sqrt{(M+N)/(\log M+N)^\sigma})$. By noting that $M \ll N$ we get that

$$C_B \ll \frac{N}{(\log N)^{\sigma/2}}.$$

This together with the estimation above yields the result. □

Finally we need an estimation for a complete exponential sum in the Gaussian rationals.

Lemma 4.7 ([36, Theorem 1])**.** *Let f be a k-th degree polynomial with coefficients in $\mathbb{Q}(i)$ and q be the least common multiple of its coefficients. If $\Lambda(q)$ is a complete set of residues modulo q, then, for any $\varepsilon > 0$,*

$$\sum_{\lambda\in\Lambda(q)} e(\operatorname{tr}(f(\lambda))) \ll (N(q))^{1-\frac{1}{k}+\varepsilon}$$

holds, where the implied constant depends only on f and ε.

4.2 Properties of the Fundamental Domain

In this section we mainly follow the paper of Gittenberger and Thuswaldner [26]. Let $b = -n+i$ be a base of a CNS in $\mathbb{Z}[i]$. Then every $\gamma \in \mathbb{C}$ has a unique representation of the shape $\gamma = \alpha + \beta b$ with $\alpha, \beta \in \mathbb{R}$. Thus we define the mapping

$$\varphi : \mathbb{C} \to \mathbb{R}^2, \quad \alpha + \beta b \mapsto (\alpha, \beta).$$

As $(1, b)$ is an integral basis we get that $\varphi(\mathbb{Z}[i]) = \mathbb{Z}^2$.

We define the *fundamental domain* $\mathcal{F}'$ to consist of all numbers with zero in the integer part of their b-ary representation. Thus

$$\mathcal{F}' := \left\{\gamma \in \mathbb{C} \middle| \gamma = \sum_{k\geq 1} d_k b^{-k}, d_k \in \mathcal{D}\right\}.$$

As it is more easy to consider the properties in $\mathbb{R}^2$ we use our embedding from above to switch from $\mathbb{C}$ to $\mathbb{R}^2$. Then we get

$$\mathcal{F} := \varphi(\mathcal{F}') = \left\{ \gamma \in \mathbb{R}^2 \,\middle|\, \gamma = \sum_{k \geq 1} d_k B^{-k}, d_k \in \varphi(\mathcal{D}) \right\}$$

where B is the matrix corresponding to the multiplication by b in $\mathbb{R}^2$ given by

$$B = \begin{pmatrix} 0 & -1-n^2 \\ 1 & -2n \end{pmatrix}.$$

(We refer the reader to [58] for more details).

Now we define for every $a \in \mathbb{Z}[i]$ the domain corresponding to the elements of $\mathcal{F}$ whose digit representation after the comma starts with the digits of the expansion of a. In particular, we set

$$\mathcal{F}_a = B^{-\ell(a)}(\mathcal{F} + \varphi(a)). \tag{4.2.1}$$

As in the case of normal numbers in the reals we need an Urysohn-function for this fundamental domain of numbers starting with a. In the reals we use a lemma due to Vinogradov (cf. Lemma 2 of [74, p.196]), in $\mathbb{C}$, however, we have to construct a corresponding version of this lemma.

For $a \in \mathcal{D}$ this has been done by Gittenberger and Thuswaldner in section 3 of [26]. As the generalization of their construction to the case of $a \in \mathbb{Z}[i]$ runs along the same lines we only state the corresponding results and leave their proofs to the reader.

Lemma 4.8 ([26, Lemma 3.1]). *For all $a \in \mathbb{Z}[i]$ and all $k \in \mathbb{N}$ there exists an axe-parallel tube $P_{k,a}$ with the following properties:*

1. *$\partial\mathcal{F}_a \subset P_{k,a}$ for all $k \in \mathbb{N}$,*
2. *$\lambda_2(P_{k,a}) = \mathcal{O}(\mu^k / |b|^{2k})$,*
3. *$P_{k,a}$ consists of $\mathcal{O}(\mu^k)$ axe-parallel rectangles with $1 < \mu < |b|^2$, each of which has Lebesgue measure $\mathcal{O}(|b|^{-2k})$.*

Here we denote by λ_2 the usual Lebesgue measure of $\mathbb{R}^2$.

In the proof of Gittenberger and Thuswaldner [26] they define for every pair (k, a) suitable axe-parallel polygons $\Pi_{k,a}$. Then they get that $d(\Pi_{k,a}, \partial\mathcal{F}_a) < c\,|b|^{-k}$, for a constant $c > 0$, where $d(\cdot,\cdot)$ denotes the Hausdorff metric, and

$$P_{k,a} := \left\{ z \in \mathbb{R}^2 \,\middle|\, \|z - \Pi_{k,a}\|_\infty \leq 2c\,|b|^{-k} \right\}. \tag{4.2.2}$$

As in [26] we denote by $I_{k,a}$ the interior of $\Pi_{k,a}$ and define f_a by

$$f_a(x, y) = \frac{1}{\Delta^2} \int_{-\Delta/2}^{\Delta/2} \int_{-\Delta/2}^{\Delta/2} \psi_a(x + \bar{x}, y + \bar{y}) d\bar{x} d\bar{y}, \tag{4.2.3}$$

where

$$\Delta := 2c_\Delta\,|b|^{-k} \tag{4.2.4}$$

with $c_\Delta > 0$ a constant and

$$\psi_a(x, y) = \begin{cases} 1 & \text{if } (x, y) \in I_{k,a} \\ \frac{1}{2} & \text{if } (x, y) \in \Pi_{k,a} \\ 0 & \text{otherwise.} \end{cases}$$

Now f_a is the desired Urysohn function for $\mathcal{F}_a$ in $\mathbb{R}^2$. We perform Fourier analysis of this function and get the following results for its coefficients.

Lemma 4.9 ([26, Lemma 3.2]). *Let $f_a(x,y)=\sum_{m,n} C(m,n)e(mx+ny)$ be the Fourier expansion of f_a. Then for the Fourier coefficients $C(m,n)$ we get the estimates*

$$C(m,n)=\begin{cases}|b|^{-2\ell(a)} & m=n=0,\\ \mu^k c(m)c(n) & \text{otherwise,}\end{cases} \tag{4.2.5}$$

where

$$c(t)\ll\begin{cases}1 & t=0,\\ \min(|t|^{-1},\Delta|t|^{-2}) & \text{otherwise.}\end{cases} \tag{4.2.6}$$

As the proof of this lemma runs along the same lines as that of [26, Lemma 3.2] we omit it.

The coefficient $C(0,0)$ will correspond to the main term and all others contribute to the error term. One of our main tools will be Weyl sums which will be discussed in the next section.

4.3 The Weyl Sum

This estimation will play a crucial rôle in the proof of the Theorem.

Throughout this section we denote by f a polynomial with coefficients in $\mathbb{C}$. Thus

$$f(z)=\alpha_d z^d+\alpha_{d-1}z^{d-1}+\cdots+\alpha_1 z.$$

In order to establish an upper bound we will generalize Lemma 2 of Nakai and Shiokawa [54].

Proposition 4.10. *Let $G>0$ be any constant and $N\geq 2$. Let s be an integer with $1\leq s\leq d$, let H_i, K_i $(i=s+1,s+2,\dots,d-1,d)$ be any positive constants, and let H_s^*, K_s^* be constants such that*

$$H_s^*\geq 2^{3s}+2^{s+1}(G+\max_{s<i\leq d}H_i)+s\sum_{i=s+1}^{d}K_i,$$

$$K_s^*\geq 2^{3s}+2^{s+1}(G+\max_{s<i\leq d}H_i)+2s\sum_{i=s+1}^{d}K_i.$$

Suppose that there are Gaussian integers a_i and q_i $(s<i\leq d)$ such that

$$1\leq|q_i|^2\leq(\log N)^{K_i}\quad\text{and}\quad\left|\alpha_i-\frac{a_i}{q_i}\right|\leq\frac{(\log N)^{H_i}}{|q_i|N^{i/2}}$$

and that there exist no Gaussian integers a_s and q_s with $(a_s,q_s)=1$ such that

$$1\leq|q_s|^2\leq(\log N)^{K_s^*}\quad\text{and}\quad\left|\alpha_s-\frac{a_s}{q_s}\right|\leq\frac{(\log N)^{H_s^*}}{|q_s|N^{s/2}}. \tag{4.3.1}$$

Then

$$\left|\sum_{|z|^2\leq N}e(\mathrm{tr}(f(z)))\right|\ll N(\log N)^{-G}$$

holds.

Before we start proving the proposition we need three lemmata. The first deals with approximation by Gaussian integers.

Lemma 4.11 ([19, Theorem 4.5]). *Given any $z=x+iy\in\mathbb{C}$ and $N\in\mathbb{N}$, there exist Gaussian integers a and q with $0<|q|^2\leq N$ such that*

$$\left|z-\frac{a}{q}\right|<\frac{2}{|q|\sqrt{N}}.$$

In order to state Weyl's inequality in that context we need a more general version of diophantine approximation in the Gaussian integers.

Lemma 4.12 ([62, Lemma 2]). *Let $h > 2$. Then for $\alpha \in \mathbb{C}$ there exist $q \in \mathbb{Z}[i]$ and $a \in \frac{1}{2}\mathbb{Z}[i]$ such that*

$$|q\alpha - a| < h^{-1}, \quad 0 < |q| \leq h,$$

$$\max(h\,|q\alpha - a|\,, |q|) \geq \frac{1}{2},$$

and

$$\mathrm{N}(2a, q)) \leq 2.$$

Furthermore we need a lemma which considers the case that $s = d$, the degree of the polynomial f, *i.e.*, that the leading coefficient is already well approximable.

Lemma 4.13. *Let $q \in \mathbb{Z}[i]$ be such as in Lemma 4.12 with $\alpha = \alpha_d$ and $h^2 = N^d(\log N)^{-H}$. If $(\log N)^H \leq |q|^2$, then we have*

$$\left| \sum_{|z|^2 < N} e\left(\mathrm{tr}(f(z))\right) \right| \ll N(\log N)^{-G}$$

with $H \geq 2^d G + 2^{3d}$.

Proof. In order to prove this one has to follow the proof of Theorem 3.2 in [80] and has to replace Lemma 3.7 of [80] by Lemma 2.5 of [26]. □

Now we can start the proof of Proposition 4.10.

Proof of Proposition 4.10. This proof mainly follows the ideas of Nakai and Shiokawa for their proof of Lemma 2 in [54].

We consider the different possibilities for s. If $s = d$ nothing is to show as this is exactly the case of Lemma 4.13.

Let $s < d$. We denote by k the least common multiple of $q_{s+1}, \ldots, q_d$. We have $k \in \mathbb{Z}[i]$ because the Gaussian integers are a unique factorization domain. We denote by Q the integer such that $|k|^2 Q \leq N < |k|^2 (Q + 1)$. By our assumptions we have that

$$1 \leq |k|^2 \leq (\log N)^K \quad \text{with } K = \sum_{i=s+1}^{d} K_i$$

and

$$N(\log N)^{-K} \ll Q \ll N / |k|^2 .$$

Now we use the fact that $\mathbb{Z}[i]$ is an Euclidean domain. From this we get that for every $s \in \mathbb{Z}[i]$ there exist unique $q, r \in \mathbb{Z}[i]$ with $|r|^2 < |k|^2$ such that $s = qk + r$. Thus we get that there exists a complete residue system R modulo k with

$$R \subset \{z \in \mathbb{Z}[i] : |z| \leq |k|\}.$$

We use this residue system to tessellate the open disc $D := \{z : |z|^2 < N\}$ with translates of R. Let T be these translates, *i.e.*,

$$T := \{t \in \mathbb{Z}[i] : (R + tk) \cap D \neq \emptyset\}.$$

Now we define I to be the translates which are completely contained in D, *i.e.*,

$$I := \{t \in T : (R + tk) \subset D\}.$$

As there are $\mathcal{O}(\sqrt{N})$ points on the circumference and there are $\mathcal{O}(|k|)$ points in R we get that

$$\sum_{|z|^2\leq N} e(\operatorname{tr}(f(z))) = \sum_{t\in I}\sum_{r\in R} e(\operatorname{tr}(f(tk+r))) + \mathcal{O}(\sqrt{N}\,|k|).$$

As in the proof of Lemma 2 of Nakai and Shiokawa in [54] we want to do Abel Summation. Therefore we need an ordering on I. Let $x, y \in I$, then define

$$x \prec y :\Leftrightarrow \begin{cases} |x| < |y| \text{ or} \\ (|x| = |y| \text{ and } \arg(x) < \arg(y)) \end{cases}$$

By the polar representation of every complex number we get that this ordering is well defined. Furthermore we set $\sigma : \mathbb{N} \to I$ a bijection such that $\sigma(1) = 0$, $\sigma(|I|) = \max I$, and

$$\sigma(x) \prec \sigma(y) :\Leftrightarrow x < y,$$

where the maximum is with respect to $\prec$. Let $M = |I|$ then we have

$$\sum_{|z|^2\leq N} e(\operatorname{tr}(f(z))) = \sum_{n=1}^{M}\sum_{r\in R} e(\operatorname{tr}(f(\sigma(n)k+r))) + \mathcal{O}(\sqrt{N}\,|k|) \tag{4.3.2}$$

Now we are ready to do Abel Summation and define for short

$$\psi_r(x) = \sum_{i=s+1}^{d} \gamma_i (xk+r)^i, \qquad \gamma_i = \alpha_i - \frac{a_i}{q_i},$$

$$\varphi_r(x) = \sum_{i=1}^{s} \alpha_i (xk+r)^i, \qquad T_r(\ell) = \sum_{n=1}^{\ell} e(\operatorname{tr}(\varphi_r(\sigma(n)))).$$

By the linearity of the trace tr we get that

$$\begin{aligned}
&\sum_{n=1}^{M}\sum_{r\in R} e(\operatorname{tr}(f(\sigma(n)k+r))) \\
&= \sum_{r\in R}\sum_{n=1}^{M} e(\operatorname{tr}(\sum_{i=1}^{d}\alpha_i(\sigma(n)k+r)^i)) \\
&= \sum_{r\in R}\sum_{n=1}^{M} e(\operatorname{tr}(\sum_{i=1}^{s}\alpha_i(\sigma(n)k+r)^i + \sum_{i=s+1}^{d}\alpha_i(\sigma(n)k+r)^i)) \\
&= \sum_{r\in R}\sum_{n=1}^{M} e(\operatorname{tr}(\varphi_r(\sigma(n)) + \sum_{i=s+1}^{d}(\gamma_i + \frac{a_i}{q_i})(\sigma(n)k+r)^i)) \\
&= \sum_{r\in R} e\left(\operatorname{tr}\left(\sum_{i=s+1}^{d}\frac{a_i}{q_i}r^i\right)\right)\sum_{n=1}^{M} e(\operatorname{tr}(\varphi_r(\sigma(n)) + \psi_r(\sigma(n)))) \qquad (4.3.3)\\
&= \sum_{r\in R} e\left(\operatorname{tr}\left(\sum_{i=s+1}^{d}\frac{a_i}{q_i}r^i\right)\right)\sum_{n=1}^{M} e(\operatorname{tr}(\psi_r(\sigma(n))))\,(T_r(n) - T_r(n-1)) \\
&= \sum_{r\in R} e\left(\operatorname{tr}\left(\sum_{i=s+1}^{d}\frac{a_i}{q_i}r^i\right)\right)\Bigg[e(\operatorname{tr}(\psi_r(\sigma(M+1))))T_r(M) \\
&\qquad + \sum_{n=1}^{M}\left(e(\operatorname{tr}(\psi_r(\sigma(n)))) - e(\operatorname{tr}(\psi_r(\sigma(n+1))))\right) T_r(n)\Bigg] \\
&\ll \sum_{r\in R}\left[|T_r(M)| + \sum_{n=1}^{M}\left|e(\operatorname{tr}(\psi_r(\sigma(n)))) - e(\operatorname{tr}(\psi_r(\sigma(n+1))))\right| |T_r(n)|\right]
\end{aligned}$$

As the trace is a linear functional we get

$$\frac{d}{dx}\operatorname{tr}(f(x)) = \operatorname{tr}\left(\frac{df}{dx}\right).$$

Noting that for $a \in \mathbb{C}$ we have $\operatorname{tr}(a) \ll |a|$ and that for $1 < n \leq M$ we get $|\sigma(n) - \sigma(n+1)| \ll N^{\frac{1}{2}}$, we apply the mean-value of calculus theorem to get

$$|e(\operatorname{tr}(\psi_r(\sigma(n)))) - e(\operatorname{tr}(\psi_r(\sigma(n+1))))| \ll |k| \sum_{i=s+1}^{d} |\gamma_i| N^{i/2-1} \ll |k| \frac{(\log N)^H}{N}$$

where $H = \max\{H_i : i = 1, \dots, s\}$.

Thus

$$\sum_{n=1}^{M} \sum_{r \in R} e(\operatorname{tr}(f(\sigma(n)k + r))) \ll \sum_{r \in R} \left[|T_r(M)| + |k| \frac{(\log N)^H}{N} \sum_{n=1}^{M} |T_r(n)| \right]. \tag{4.3.4}$$

If we can show that

$$|T_r(n)| \ll \frac{N}{|k| (\log N)^{G+H}} \tag{4.3.5}$$

then we are done. We may assume that

$$n \gg \frac{N}{|k| (\log N)^{G+H}}. \tag{4.3.6}$$

We split the estimation of $T_r(n)$ up, according to whether there exist a and q with $(a, q) = 1$ such that

$$(\log N)^{H'} \leq |q|^2 \leq N^s (\log N)^{-H'} \tag{4.3.7}$$

and

$$\left| k^s \alpha_s - \frac{a}{q} \right| \leq |q|^2,$$

with $H' = 2^{3s} + 2^{s+1}(G + H) + sK$, or not.

- Suppose there exist such a and q. Then by the definition of H' together with (4.3.6) we get that
$$(\log n)^{h'} \leq |q|^2 \leq n^s (\log n)^{-h'},$$
where $h' = 2^{3s} + 2^s(G + H)$. Thus an application of Lemma 4.13 yields
$$|T_r(n)| \ll n(\log n)^{-(G+H)} \ll \frac{N}{|k| (\log N)^{(G+H)}}.$$

- On the contrary if there are no such a and q then we get by Lemma 4.12 that there must exist a and q with $(a, q) = 1$ and $|q|^2 \leq N^s (\log N)^{-H'}$. Thus we get by (4.3.7) that
$$1 \leq |q|^2 \leq (\log N)^{-H'} \quad \text{and} \quad \left| k^s \alpha_s - \frac{a}{q} \right| \leq \frac{(\log N)^{-H'/2}}{|q| N^{s/2}}.$$
Then, however, we get
$$|k^s q|^2 \leq (\log N)^{H'+sK} \leq (\log N)^{K_s^*},$$
and thus
$$\left| \alpha_s - \frac{a}{k^s q} \right| \leq \frac{(\log N)^{H_s^*}}{|k|^s |q| N^s},$$
which contradicts the assumption on α_s.

Therefore we have shown (4.3.5). Thus we get together with (4.3.2) and (4.3.4) that

$$\begin{aligned}\sum_{|z|^2\leq N} e(\mathrm{tr}(f(z))) &\ll \sum_{r\in R}\left[|T_r(M)| + |k|\frac{(\log N)^H}{N}\sum_{n=1}^{M}|T_r(n)|\right] + \sqrt{N}\,|k| \\ &\ll \sum_{r\in R}\left[\frac{N}{|k|\,(\log N)^{G+H}} + \frac{1}{(\log N)^G}M\right] + \sqrt{N}\,|k| \\ &\ll \frac{N}{(\log N)^G}\end{aligned}$$

and the proposition is proven. □

Now we have enough tools to proceed to the proof of the main theorem.

4.4 Proof of Theorem 4.1

In the rest of this chapter we will consider the proof of Theorem 4.1. The proof will split up into several parts.

1. We start in Section 4.4.1 with a definition of several parameters which will be useful in the proof. Furthermore we show some connections between them.
2. Then in Section 4.4.2 we rewrite the problem into one of an estimation of an exponential sum. This sum is finally transfered into one of type as in Proposition 4.10 or Lemma 4.13.
3. We consider these sums according to the b-ary length of their arguments. There will be no problem when considering the middle ones in Section 4.4.3. By middle we mean that there exists a upper and lower bound for the b-ary length of the expansion. For those arguments with a long or short expansion we have to use different methods in Sections 4.4.4 and 4.4.5, respectively.
4. Finally we put everything together and get the result.

Throughout the proof we will fix N and the block $d_1 \dots d_l$ under consideration. Furthermore we set

$$a := \sum_{i=1}^{l} d_i b^{l-i} \tag{4.4.1}$$

for abbreviation.

4.4.1 Defining parameters and explaining relations between them

Let m be the unique positive integer such that

$$\sum_{n\leq m-1}\ell(f(z_n)) < N \leq \sum_{n\leq m}\ell(f(z_n)), \tag{4.4.2}$$

where $z_n := \tau^{-1}(n-1)$ with $n \geq 1$. Furthermore we denote by M the maximum norm and by J the maximum length of the $(b,\mathcal{D})$-ary expansion of $\lfloor f(z_n)\rfloor$ for $1 \leq n \leq m$, *i.e.*,

$$M := \max_{n\leq m}|z_n|^2, \quad J := \max_{n\leq m}\ell(f(z_n)).$$

These will be of central interest for us.

Now we will use Lemma 4.2 to connect m and M. We get

$$\left|\log_{|b|^2} \max_{n\le m} |z_n|^2 - \ell(\max_{n\le m} z_n)\right| = \left|\log_{|b|^2} M - \ell(z_m)\right| = \left|\log_{|b|^2} M - \left\lfloor \log_{|b|^2} m \right\rfloor\right| \le c,$$
$$M \ll\gg m,$$

where $\ll\gg$ means both $\ll$ and $\gg$.

For the connection of M and J we note that $|f(z)| \ll\gg |z|^d$. Thus we get by Lemma 4.2 that

$$\begin{gathered}\left|\log_{|b|^2} \max_{n\le m} |f(z_n)|^2 - J\right| \ll\gg \left|\log_{|b|^2} \max_{n\le m} |z_n|^{2d} - J\right| = \left|\log_{|b|^2} M^d - J\right|, \\ M \ll\gg |b|^{2\frac{J}{d}} \le c.\end{gathered} \tag{4.4.3}$$

Finally we get the following relation between M and N.

$$N = mJ + \mathcal{O}(m) = c_0 M \log_q M + \mathcal{O}(M),$$

where c_0 is a positive constant depending on d and b.

Next we want to split the sum on the right of (4.4.2) up into parts where $f(z_n)$ has the same b-ary length. Therefore let $I_l, I_{l+1}, I_{l+2}, \dots, I_J \subset \{1, \dots, m\}$ be such that

$$n \in I_j :\Longleftrightarrow \ell(f(z_n)) \ge j.$$

In order to estimate the size of these subsets we define M_j $(j = l, l+1, \dots, J)$ to be the least integers such that any $z \in \mathbb{C}$ of norm greater or equal M_j has at least length j, *i.e.*,

$$M_j := \max_{\ell(z)<j} |z|^2 = \max_{n<|b|^{2(j-1)}} |z_n|^2.$$

By the same arguments as in (4.4.3) we get that $M_j \ll\gg |b|^{2\frac{j}{d}}$. Furthermore we set

$$X_j := M - M_j. \tag{4.4.4}$$

4.4.2 Rewriting the problem

With the help of the parameters defined above we can easily rewrite our problem. Therefore we set $\mathcal{N}(f(z_n))$ the number of occurrences of the block $d_1 \dots d_l$ in the b-ary expansion of the integer part of $\lfloor f(z_n) \rfloor$. Then we get that

$$\left|\mathcal{N}(\theta_q(f); d_1 \dots d_\ell, N) - \sum_{n\le m} \mathcal{N}(f(z_n))\right| \le 2lm.$$

Thus it suffices to show that

$$\sum_{n\le m} \mathcal{N}(f(z_n)) = \frac{N}{|\mathcal{D}|^l} + \mathcal{O}\left(\frac{N}{\log N}\right). \tag{4.4.5}$$

In order to count the occurrences of the block $d_1 \dots d_l$ in $\lfloor f(z_n) \rfloor$ properly we define the indicator function of $\mathcal{F}_a$ (where a is as in (4.4.1) and $\mathcal{F}_a$ is defined in (4.2.1))

$$\mathcal{I}_a(z) = \begin{cases} 1 & z \in \mathcal{F}_a, \\ 0 & \text{otherwise.} \end{cases}$$

Indeed, writing $f(z_n)$ in $(b, \mathcal{D})$-ary expansion for a fixed $n \in \{1, \dots, m\}$, *i.e.*,

$$f(z_n) = a_r b^r + a_{r-1} b^{r-1} + \dots + a_1 b + a_0 + a_{-1} b^{-1} + \dots,$$

with $a_i \in \mathcal{D}$ for $i = r, r-1, \dots$, we see that the function $\mathcal{I}(z_n)$ is defined such that

$$\mathcal{I}(b^{-j-1} f(z_n)) = 1 \Longleftrightarrow d_1 \dots d_l = a_{j-1} \dots a_{j-l}.$$

As every I_j ($l \leq j \leq J$) consists of exactly those $f(z_n)$ whose $(b, \mathcal{D})$-ary expansion has at least length j, we get that

$$\sum_{n \leq m} \mathcal{N}(f(z)) = \sum_{l \leq j \leq J} \sum_{n \in I_j} \mathcal{I}\left(\frac{f(z_n)}{b^{j+1}}\right).$$

For every j there can be elements $z \in \mathbb{Z}[i]$ with $|z|^2 < M_j$ but $\ell(z) \geq j$. By Lemma 4.2 we get that there are only finitely many with this property. Now by Lemma 2.6 we get that

$$\sum_{n \in I_j} 1 = \sum_{|z_n| < M_j} 1 + \sum_{M_j \leq |z_n|^2 < M} 1 \sim \sum_{M_j \leq |z_n|^2 < M} 1.$$

Therefore we can assume that there are no z with $\ell(z) \geq j$ and $|z|^2 < M_j$.

In order to estimate $\mathcal{I}(z)$ we use our considerations of Section 4.2. Noting that $\mathcal{F}_a$ can be covered by a set $I_{k,a}$ and an axe parallel tube $P_{k,a}$ (*cf.* (4.2.2)), we have to consider how often the sequence $\left\{b^{-j-1} f(z_n)\right\}_{n \in I_j}$ hits each of these sets. The first one, $I_{k,a}$, is characterized by the Urysohn function $f_a(x, y)$ (*cf.* (4.2.3)) and for the axe-parallel tube we define

$$\mathcal{E}_j := \#\left\{n \in I_j : \varphi\left(\frac{f(z_n)}{b^{j+1}}\right) \in P_{k,a}\right\}.$$

Thus we get for every $j \in \{l, l+1, \dots, J\}$ that

$$\sum_{n \in I_j} \mathcal{I}\left(\frac{f(z_n)}{b^{j+1}}\right) = \sum_{n \in I_j} f_a\left(\varphi\left(\frac{f(z_n)}{b^{j+1}}\right)\right) + \mathcal{O}\left(\mathcal{E}_j\right). \tag{4.4.6}$$

We consider both terms on the right hand side of (4.4.6) separately starting with f_a and get by Lemma 4.9 that

$$f_a\left(\varphi\left(\frac{f(z_n)}{b^{j+1}}\right)\right) = |b|^{-2\ell(a)} + \sum_{\mathbf{0} \neq \boldsymbol{v} \in \mathbb{Z}^2} C(v_1, v_2)\, e\left(\boldsymbol{v} \cdot \varphi\left(\frac{f(z_n)}{b^{j+1}}\right)\right),$$

where $\boldsymbol{v} = (v_1, v_2)$ and $C(\cdot, \cdot)$ is defined as in (4.2.5).

By the estimations of the Fourier coefficients in (4.2.6) we can split the sum up into those $\boldsymbol{v}$ with $\|\boldsymbol{v}\|_\infty \leq \Delta^{-1}$ and the rest. For $\|\boldsymbol{v}\|_\infty > \Delta^{-1}$ we apply our estimate for the coefficients in (4.2.6) and estimate the $e(\cdot)$ function trivially to get

$$\sum_{n \in I_j} f_a\left(\varphi\left(\frac{f(z_n)}{b^{j+1}}\right)\right) \ll \frac{X_j}{|b|^{2l}} + X_j \mu^k \Delta^2 + \mu^k \sum_{\mathbf{0} < \|\boldsymbol{v}\|_\infty \leq \Delta^{-1}} \frac{1}{r(\boldsymbol{v})} \sum_{n \in I_j} e\left(\boldsymbol{v} \cdot \varphi\left(\frac{f(z_n)}{b^{j+1}}\right)\right). \tag{4.4.7}$$

To estimate $\mathcal{E}_j$ we use the Erdos-Turan-Koksma inequality (Lemma 4.3). By Lemma 4.8 we can split the tube $P_{k,a}$ into a family of μ^k rectangles $\boldsymbol{R}_j$. As the discrepancy is defined on a rectangle (*cf.* [21, p.5]) we get by an application of Lemma 4.3 that

$$\begin{aligned}\mathcal{E}_j &\ll \sum_{\boldsymbol{R}_j} X_j \lambda_2(R) + X_j D_{X_j}(\{x_n\}) \\ &\ll X_j \sum_{\boldsymbol{R}_j} \left(\lambda_2(R) + \frac{2}{H+1} + \sum_{0 < \|\boldsymbol{h}\|_\infty \leq H} \frac{1}{r(\boldsymbol{v})} \left|\frac{1}{X_j} \sum_{n \in I_j} e\left(\boldsymbol{v} \cdot \varphi\left(\frac{f(z_n)}{b^{j+1}}\right)\right)\right|\right),\end{aligned} \tag{4.4.8}$$

where the sum is extended over all rectangles R comprising the tube $P_{k,a}$ can be split into.

By the property (3) of $P_{k,a}$ described in Lemma 4.8 and possible overlappings of the rectangles in $\boldsymbol{R_j}$ we get that

$$\sum_{\boldsymbol{R}_j} \lambda_2(R) \ll \left(\frac{\mu}{|b|^2}\right)^k.$$

Thus (4.4.8) simplifies to

$$\mathcal{E}_j \ll X_j \left(\left(\frac{\mu}{|b|^2}\right)^k + \frac{\mu^k}{H+1} + \frac{\mu^k}{X_j} \sum_{0<\|\boldsymbol{v}\|_\infty \le H} \frac{1}{r(\boldsymbol{v})} \sum_{n \in I_j} S(\boldsymbol{v}, j)\right). \tag{4.4.9}$$

As both exponential sums in (4.4.7) and (4.4.8) are of the same shape, we define for short

$$S(\boldsymbol{v}, j) := \sum_{n \in I_j} e\left(\boldsymbol{v} \cdot \varphi\left(\frac{f(z_n)}{b^{j+1}}\right)\right). \tag{4.4.10}$$

Plugging (4.4.7), (4.4.9), and (4.4.10) in (4.4.6) and subtracting the mayor part we get

$$\left|\sum_{n \in I_j} \mathcal{I}\left(\frac{f(z_n)}{b^{j+1}}\right) - \frac{X_j}{|b|^{2l}}\right| \ll$$

$$X_j \left(\mu^k \Delta^2 + \frac{2\mu^k}{H+1} + \left(\frac{\mu}{|b|^2}\right)^k\right) + \sum_{\boldsymbol{0}<\|\boldsymbol{v}\|_\infty \le \Delta^{-1}} \frac{\mu^k}{r(\boldsymbol{v})} S(\boldsymbol{v}, j) + \sum_{0<\|\boldsymbol{v}\|_\infty \le H} \frac{\mu^k}{r(\boldsymbol{v})} S(\boldsymbol{v}, j). \tag{4.4.11}$$

In order to transfer the exponential sum from $\mathbb{Z}^2$ to $\mathbb{Z}[i]$ we use the same idea as Gittenberger and Thuswaldner in [26, p.335]. Thus let

$$\tau(z) := (\operatorname{tr} z, \operatorname{tr} bz)^t = \Xi\varphi(z),$$

where $\Xi = VV^t$ an V is the Vandermonde matrix

$$V = \begin{pmatrix} 1 & 1 \\ b & \overline{b} \end{pmatrix}.$$

By this we get that

$$\boldsymbol{v} \cdot \varphi\left(\frac{f(z)}{b^{j+1}}\right) = \boldsymbol{v}\Xi^{-1}\tau\left(\frac{f(z)}{b^{j+1}}\right) = \operatorname{tr}\left((\widetilde{v_1} + b\widetilde{v_2})\frac{f(z)}{b^{j+1}}\right),$$

where $(\widetilde{v_1}, \widetilde{v_2}) := \boldsymbol{v}\Xi^{-1}$.

Thus we get that (4.4.10) transfers to

$$\begin{aligned} S(\boldsymbol{v}, j) &= \sum_{n \in I_j} e\left(\operatorname{tr}\left((\widetilde{v_1} + b\widetilde{v_2})\frac{f(z_n)}{b^{j+1}}\right)\right) \\ &\ll \sum_{M_j \le |z|^2 < M_j + X_j} e\left(\operatorname{tr}\left((\widetilde{v_1} + b\widetilde{v_2})\frac{f(z)}{b^{j+1}}\right)\right), \end{aligned} \tag{4.4.12}$$

where we have used that $|I_j| \ll\gg X_j$ together with the definition of X_j in (4.4.4).

We assume that we take k and H such that $\Delta^{-1}, H \ll (\log N)$, which is possible since Δ depends on k (*cf.* (4.2.4)). The value of k and H is chosen later depending on j.

In the following subsections we want to consider the different sums $S(\boldsymbol{v}, j)$ according to the size of j. We therefore split the area into three intervals as follows

$$l \le j \le l + C_l \log\log N, \tag{4.4.13}$$

$$l + C_l \log\log N < j \le J - C_u \log\log N, \tag{4.4.14}$$

$$J - C_u \log\log N < j \le J, \tag{4.4.15}$$

where C_l and C_u are sufficiently large constants.

4.4.3 A first estimation of $S(\boldsymbol{v}, j)$

We will start with the j satisfying (4.4.14).

Assume first that there are two Gaussian integers a and q such that

$$\left|\frac{\widetilde{v_1}+b\widetilde{v_2}}{b^j}\alpha_d-\frac{a}{q}\right|\leq\frac{1}{|q|^2}\quad\text{and}\quad(\log X_j)^H\leq|q|^2\leq X_j^d(\log X_j)^{-H}, \tag{4.4.16}$$

with $G=3$ and $H=2^{d+2}G+2^{3(d+2)}$. Then we apply Lemma 4.13 and get

$$S(\boldsymbol{v},j)\ll X_j(\log X_j)^{-G}.$$

Now we will show that (4.4.16) holds for all j satisfying (4.4.14).

If (4.4.16) does not hold, then we get by an application of Lemma 4.11 that there are $a,q\in\mathbb{Z}[i]$ such that

$$(a,q)=1,\quad 1\leq|q|^2\leq X_j^d(\log X_j)^{-H},\quad\text{and}\quad\left|\frac{\widetilde{v_1}+b\widetilde{v_2}}{b^j}\alpha_d-\frac{a}{q}\right|\leq\frac{(\log X_j)^H}{|q|\,X_j^{\frac{d}{2}}}\leq\frac{1}{|q|^2}.$$

We distinguish two cases for the size of $|q|^2$. Assume first that $2\leq|q|^2\leq(\log X_j)^H$. Thus we get

$$\left|\frac{\widetilde{v_1}+b\widetilde{v_2}}{b^j}\alpha_d\right|>\frac{1}{|q|}-\frac{1}{|q|^2}\geq\frac{1}{2\,|q|}\gg(\log X_j)^{-H}$$

and therefore

$$|b|^j\ll|(\widetilde{v_1}+b\widetilde{v_2})\alpha_d|\,(\log X_j)^H\ll(\log N)(\log X_j)^H,$$

which contradicts (4.4.14) for C_l sufficiently large.

We will denote by $\|z\|$ the distance of the norm of z over $\mathbb{Q}$ to the nearest integer, *i.e.*,

$$\|z\|:=\min_{n\in\mathbb{Z}}\left||z|^2-n\right|.$$

Now if $|q|^2=1$ then $q=1$ and $\left\|(\widetilde{v_1}+b\widetilde{v_2})(b^{-j})\alpha_d\right\|<X_j^d(\log X_j)^{-2H}$. If $\left|(\widetilde{v_1}+b\widetilde{v_2})(b^{-j})\alpha_d\right|^2>\frac{\sqrt{2}}{2}$ then

$$|b|^{2j}\ll|(\widetilde{v_1}+b\widetilde{v_2})\alpha_d|\ll\log N,$$

which contradicts (4.4.14) for C_l sufficiently large.

On the other hand if $\left|(\widetilde{v_1}+b\widetilde{v_2})b^{-j}\alpha_d\right|<\frac{\sqrt{2}}{2}$ we get that

$$\left|(\widetilde{v_1}+b\widetilde{v_2})b^{-j}\alpha_d\right|^2=\left\|(\widetilde{v_1}+b\widetilde{v_2})b^{-j}\alpha_d\right\|<X_j^d(\log X_j)^{-2H},$$

which implies that

$$|b|^{2j}\gg|(\widetilde{v_1}+b\widetilde{v_2})\alpha_d|^2\,X_j^d(\log X_j)^{-2H}$$

contradicting our assumption on C_u in (4.4.14).

Thus for j such that (4.4.14) holds we get

$$S(\boldsymbol{v},j)\ll X_j(\log X_j)^{-G}. \tag{4.4.17}$$

Plugging this into (4.4.11) we get that

$$\begin{aligned}\left|\sum_{n\in I_j}\mathcal{I}\left(\frac{f(z_n)}{b^{j+1}}\right)-\frac{X_j}{|b|^{2l}}\right|\ll X_j&\left(\mu^k\Delta^2+\frac{\mu^k}{V+1}+\left(\frac{\mu}{|b|^2}\right)^k\right.\\&\left.+\frac{\mu^k}{(\log X_j)^3}\left\{\sum_{\boldsymbol{0}<\|\boldsymbol{v}\|_\infty\leq\Delta^{-1}}+\sum_{0<\|\boldsymbol{v}\|_\infty\leq V}\right\}\frac{1}{r(\boldsymbol{v})}\right)\end{aligned} \tag{4.4.18}$$

Now we can choose k and H under the assumption that both are $\ll (\log N)$. Thus we set for j as in (4.4.14) together with the definition of Δ in (4.2.4) that

$$k := C_k \log\log X_j, \quad H := \mu^k \log X_j, \quad \Delta^{-1} = \frac{(\log X_j)^{C_k \log|b|}}{2c_\Delta}, \tag{4.4.19}$$

for C_k an arbitrary constant. Furthermore we define $C_\mu > 1$ to be such that

$$C_\mu \mu = |b|^2 .$$

By our setting we get for j as in (4.4.14) that

$$\left| \sum_{n\in I_j} \mathcal{I}\left(\frac{f(z_n)}{b^{j+1}}\right) - \frac{X_j}{|b|^{2l}} \right| \ll X_j \left((\log X_j)^{-1} + (\log X_j)^{-2}(\log\log X_j)^2\right) \ll \frac{X_j}{j} \tag{4.4.20}$$

for j as in (4.4.14).

Now we will show, that we get the same estimate for the other smaller and larger j.

4.4.4 Estimating the exponential sum for long b-ary expansion

In view of (4.4.14) we now concentrate on values for j satisfying (4.4.15).

In this case we start with the same assumptions for Δ^{-1} and H as above, *i.e.* $\Delta^{-1}, H \ll (\log N)$.. Thus for every j such that (4.4.16) holds we get by an application of Lemma 4.13

$$S(\boldsymbol{v}, j) \ll X_j (\log X_j)^{-G}.$$

Otherwise, if (4.4.16) does not hold we get for every j in (4.4.15) together with $|b|^{\frac{j}{d}} \ll X_j \ll |b|^{\frac{J}{d}}$ that

$$0 \ll |\widetilde{v_1} + b\widetilde{v_2}|\, |b|^{-\frac{j}{2d}} \ll |f'(z)| \ll |\widetilde{v_1} + b\widetilde{v_2}|\, |b|^{J-j-\frac{j}{2d}} \ll |\widetilde{v_1} + b\widetilde{v_2}|\, |b|^{-\frac{j}{2d}} (\log N)^{\widetilde{C_2}}. \tag{4.4.21}$$

Now we use the inequalities (4.4.21) to apply Lemma 4.6 with

$$F = \operatorname{tr}\left((\widetilde{v_1} + b\widetilde{v_2}) \frac{f(z_n)}{b^{j+1}} \right),$$

$m = |\widetilde{v_1} + b\widetilde{v_2}|\, |b|^{-\frac{j}{d}}$, and $\delta = |\widetilde{v_1} + b\widetilde{v_2}|\, |b|^{-\frac{j}{d}} (\log N)^{\widetilde{C_2}}$. Thus for j as in (4.4.15) we get with $\sigma = 2G$ that

$$\begin{aligned} S(\boldsymbol{v}, j) &\ll \frac{\sqrt{X_j}}{|\widetilde{v_1} + b\widetilde{v_2}|\, |b|^{-\frac{j}{d}}} + \frac{X_j}{(\log X_j)^{\sigma/2}} + s\left(\frac{3-\delta}{1-\delta}\right)\sqrt{X_j (\log X_j)^\sigma} \\ &\ll \frac{\sqrt{X_j}\, |b|^{\frac{j}{d}}}{|\widetilde{v_1} + b\widetilde{v_2}|} + \frac{X_j}{(\log X_j)^G}. \end{aligned} \tag{4.4.22}$$

Plugging this into (4.4.11) yields

$$\begin{aligned} \left| \sum_{n\in I_j} \mathcal{I}\left(\frac{f(z_n)}{b^{j+1}}\right) - \frac{X_j}{|b|^{2l}} \right| \ll & X_j \left(\mu^k \Delta^2 + \frac{2\mu^k}{H+1} + \left(\frac{\mu}{|b|^2}\right)^k \right. \\ & \left. + \frac{\mu^k}{X_j} \left\{ \sum_{\boldsymbol{0}<\|\boldsymbol{v}\|_\infty \le \Delta^{-1}} + \sum_{\boldsymbol{0}<\|\boldsymbol{v}\|_\infty \le H} \right\} \frac{1}{r(\boldsymbol{v})} \left(\frac{\sqrt{X_j}\, |b|^{\frac{j}{d}}}{|\widetilde{v_1} + b\widetilde{v_2}|} + \frac{X_j}{(\log X_j)^3} \right) \right). \end{aligned} \tag{4.4.23}$$

Now we set k and H and get together with (4.2.4) that

$$k := \max\left(1, \frac{\frac{1}{2}\log X_j + \log 4C_\Delta^2 - \frac{j}{d}\log|b|}{\log C_\mu}\right), \quad H := \mu^k \log X_j, \quad \Delta^{-1} = \frac{|b|^k}{2c_\Delta}.$$

This yields

$$\mu^k\Delta^2 = \frac{|b|^{\frac{j}{d}}}{\sqrt{X_j}}, \quad \mu^k \leq |b|^{2k} \ll \left(\frac{X_j}{|b|^{\frac{2j}{d}}}\right)^{\frac{\log|b|}{\log C_\mu}}, \quad \left(\frac{\mu}{|b|^2}\right)^k = \frac{1}{C_\mu^k} \ll \frac{|b|^{\frac{j}{d}}}{\sqrt{X_j}}.$$

Furthermore we get that

$$|\widetilde{v_1} + b\widetilde{v_2}| = \left|(1,b)(v_1,v_2)^t\Xi^{-1}\right| \gg \left|(v_1,v_2)^t\right| \gg \sqrt{v_1 v_2}.$$

Putting all this in (4.4.23) yields

$$\left|\sum_{n\in I_j}\mathcal{I}\left(\frac{f(z_n)}{b^{j+1}}\right) - \frac{X_j}{|b|^{2l}}\right| \ll \sqrt{X_j}\,|b|^{\frac{j}{d}} + \frac{X_j}{j} + \left(\frac{X_j}{|b|^{\frac{2j}{d}}}\right)^{\frac{\log|b|}{\log C_\mu}}\left(\sqrt{X_j}\,|b|^{\frac{j}{d}} + X_j(\log X_j)^{-3}\right) \tag{4.4.24}$$

for j as in (4.4.15).

4.4.5 Iterative estimation for short b-ary expansion

We finally consider the case of j satisfying (4.4.13). This will be the hardest part as by our assumptions on H and Δ^{-1} we have

$$|\widetilde{v_1} + b\widetilde{v_2}| \ll\gg |b|^j.$$

In order to cope with this we adopt the idea of Nakai and Shiokawa [54, p.278ff] applying Proposition 4.10 iteratively. If there is no such s as assumed in that proposition, we will apply Lemma 4.6 and Lemma 4.7.

By the assumption $j \leq l + C_l \log\log N$ we get

$$|b|^j \leq (\log N)^{C_l \log|b| + o(1)}. \tag{4.4.25}$$

Furthermore we define g to be the polynomial

$$g(z) := \frac{\widetilde{v_1} + b\widetilde{v_2}}{b^j} f(z),$$

and β_i for $i = 0, 1, \ldots, d$ its coefficients,

$$\beta_i = \frac{\widetilde{v_1} + b\widetilde{v_2}}{b^j}\alpha_i. \tag{4.4.26}$$

Now we start with the application of Proposition 4.10. We assume first that $1 \leq s \leq d$. Then we set

$$H_d = H_d^* + C_1\log|b| + 1, \quad H_d^* = 2^{3(d+2)} + 2^{d+3}G$$

and define H_r^*, H_r, and h_r $(1 \leq r < d)$ inductively by

$$H_r^* = 2^{3(r+2)} + 2^{r+3}(G + H_{r+1}) + 2r\sum_{i=r+1}^{d} H_r,$$

$$H_r = H_r^* + 2(C_1 \log |b| + 1) \quad \text{and}$$
$$h_r = H_r^* + C_1 \log |b| + 1.$$

Let j be such that $l \le j \le l + C_l \log\log N$ and that there are coprime pairs of Gaussian integers $(a_d, q_d), \dots, (a_{s+1}, q_{s+1})$ such that

$$1 \le |q_r|^2 \le (\log X_j)^{2h_r} \quad \text{and} \quad \left|\alpha_r - \frac{a_r}{q_r}\right| \le \frac{(\log X_j)^{h_r}}{|q_r|\, X_j^{\frac{r}{2}}} \quad (s < r \le d),$$

but there is no pair (a_s, q_s) such that

$$1 \le |q_s|^2 \le (\log X_j)^{2h_s} \quad \text{and} \quad \left|\alpha_s - \frac{a_s}{q_s}\right| \le \frac{(\log X_j)^{h_s}}{|q_s|\, X_j^{\frac{s}{2}}}.$$

We denote the set of all j with that property by $\mathbb{J}_s$.

For every $j \in \mathbb{J}_s$ we have

$$1 \le \left|b^j q_r\right| \le (\log X_j)^{2H_r} \quad \text{and} \quad \left|\beta_r - \frac{(\widetilde{v_1} + b\widetilde{v_2})a_r}{b^j q_r}\right| \le \frac{(\log X_j)^{H_r}}{|b^j q_r|\, X_j^{\frac{r}{2}}}$$

for $s < r \le d$, and, however, there is no pair of coprime Gaussian integers (A_s, Q_s) such that

$$1 \le |Q_s| \le (\log X_j)^{2H_s^*} \quad \text{and} \quad \left|\beta_r - \frac{A_s}{Q_s}\right| \le \frac{(\log X_j)^{H_s^*}}{|Q_s|\, X_j^{\frac{s}{2}}},$$

since, if there were such A_s and Q_s, we would get that

$$1 \le |(\widetilde{v_1} + b\widetilde{v_2})Q_s|^2 \le (\log X_j)^{2H_s^* + t} \le (\log X_j)^{2h_s}$$

and together with (4.4.25) that

$$\left|\alpha_s - \frac{b^j A_s}{\widetilde{v_1} + b\widetilde{v_2} Q_s}\right| \le \frac{(\log X_j)^{H_s^* + C_1 \log|b| + 1}}{|(\widetilde{v_1} + b\widetilde{v_2})Q_s|\, X_j^{\frac{s}{2}}} \le \frac{(\log X_j)^{h_s}}{|(\widetilde{v_1} + b\widetilde{v_2})Q_s|\, X_j^{\frac{s}{2}}},$$

which contradicts the assumption that $j \in \mathbb{J}_s$.

Thus an application of Proposition 4.10 with H_i, H_s^* and $K_i = 2H_i$, $K_i^* = 2H_i^*$ yields

$$S(\boldsymbol{v}, j) \ll X_j (\log X_j)^{-G}$$

for all $j \in \mathbb{J}_1 \cup \dots \cup \mathbb{J}_d$.

Now we denote by $\mathbb{J}_0$ all positive integers j with $l \le j \le l + C_1 \log\log N$ and $j \notin \mathbb{J}_1 \cup \dots \cup \mathbb{J}_d$. Thus it remains to estimate $S(\boldsymbol{v}, j)$ for these j. Therefore we will apply Lemma 4.6 and the Lemma 4.7.

For $j \in \mathbb{J}_0$ we get that there exist coprime pairs (a_r, q_r) of Gaussian integers such that

$$1 \le |q_r|^2 \le (\log X_j)^{2h_r} \quad \text{and} \quad \left|\alpha_r - \frac{a_r}{q_r}\right| \le \frac{(\log X_j)^{h_r}}{|q_r|\, X_j^{\frac{r}{2}}} \quad (1 \le r \le d).$$

We set $\Omega_r = \alpha_r - \frac{a_r}{q_r}$ for $r = 1, \dots, d$. Furthermore we denote by a the greatest common divisor of $a_1, \dots, a_d$ and by q the least common multiple of $q_1, \dots, q_d$. Furthermore we define c_r by

$$\frac{a_r}{q_r} = \frac{a}{q} c_r \quad (r = 1, \dots, d).$$

Then we can rewrite the exponential sum as follows:

$$S(\boldsymbol{v}, j) = \sum_{n \in I_j} e\left(\operatorname{tr}\left((\widetilde{v_1} + b\widetilde{v_2})\frac{f(z_n)}{b^{j+1}}\right)\right)$$

$$= \sum_{\lambda \in r(b^{j+1}q)} e\left(\operatorname{tr}\left(\frac{\hat{v}a}{b^{j+1}q}\sum_{k=1}^{d} c_k\lambda^k\right)\right) \sum_{\substack{\mu \\ \exists n\in I_j : \mu q+\lambda = z_n}} e\left(\operatorname{tr}\left(\frac{\hat{v}}{b^{j+1}}\sum_{k=1}^{d}\Omega_k(\mu q+\lambda)^k\right)\right)$$

where $r(b^{j+1}q)$ denotes a complete system of residues modulo $b^{j+1}q$ and $\hat{v} := \widetilde{v_1} + b\widetilde{v_2}$.

We first consider the second sum. Let $R_0 = \mathbb{Z}[i] \cap (b^{j+1}q) \cdot \{\alpha + \beta i : 0 \leq \alpha, \beta \leq 1\}$ and let T_0 the set of translates such that R_0 tiles $\mathbb{Z}^2$. Furthermore we set T the set of all $t \in T_0$ that do not have empty intersection with I_j, thus

$$T := \{t \in T_0 : (R_0 + t) \cap \{z_n : n \in I_j\} \neq \emptyset\}. \tag{4.4.27}$$

Then it is clear that $|T| \ll X_j \left|b^{j+1}q\right|^{-2}$. Furthermore let $\mathcal{T}$ denote the area covered by the translates of T, *i.e.*,

$$\mathcal{T} := \bigcup_{t \in T} (R_0 + t).$$

Thus we fix a $\lambda \in R_0$ and get that

$$\sum_{\substack{\mu \\ \exists n\in I_j : \mu q+\lambda = z_n}} e\left(\operatorname{tr}\left(\frac{\hat{v}}{b^{j+1}}\sum_{k=1}^{d}\Omega_k(\mu q+\lambda)^k\right)\right) \leq \sum_{\mu \in T} e\left(\operatorname{tr}\left(\frac{\hat{v}}{b^{j+1}}\sum_{k=1}^{d}\Omega_k(\mu q+\lambda)^k\right)\right).$$

Now we want to apply Lemma 4.5 together with the idea in the proof of Lemma 4.6. Therefore we set

$$F_\lambda(x,y) := e\left(\operatorname{tr}\left(\frac{\hat{v}}{b^{j+1}}\sum_{k=1}^{d}\Omega_k((x+iy)q+\lambda)^k\right)\right).$$

Then we get for the derivatives

$$\frac{\partial F_\lambda(x,y)}{\partial x} \ll\gg \frac{\partial F_\lambda(x,y)}{\partial y} \ll \frac{\hat{v}}{|b|^j}\sum_{k=1}^{d} k\,|q|\,\frac{(\log X_j)^{H_k}}{q_k X_j^{k/2}} X_j^{\frac{k-1}{2}} \ll \frac{\hat{v}}{|b|^j} X_j^{-\frac{1}{2}}\,|q|\,(\log X_j)^{H_1^*}.$$

As in the proof of Lemma 4.6 we first consider a single square. We denote by $D_\nu := \{z = x + iy \in \mathbb{Z}[i] : -\nu \leq x, y \leq \nu\}$. Thus an application of Lemma 4.5 yields

$$\sum_{x+iy \in D_\nu} F_\lambda(x,y) = \sum_{x=-\nu}^{\nu}\sum_{y=-\nu}^{\nu} F_\lambda(x,y) = \int_{-\nu}^{\nu}\int_{-\nu}^{\nu} F_\lambda(x,y)\mathrm{d}x\mathrm{d}y + \mathcal{O}(\nu).$$

Now we again want to split $\mathcal{T}$ up into squares. Therefore we note that we had assumed that $|I_j| = X_j$ and thus we can consider I_j as an annulus, *i.e.* as set $\{z \in \mathbb{C} : M_j \leq |z|^2 < M\}$. Thus we choose a $\sigma > 0$ and tessellate $\mathcal{T}$ by squares of side length $\sqrt{|T|/(\log|T|)^\sigma}$. Then we can glue all squares in the interior of $\mathcal{T}$ together and estimating their contribution on the boundary to the error term. Thus we get

$$\sum_{x+iy \in T} F_\lambda(x,y) = \iint_{\mathcal{T}} F_\lambda(x,y)\mathrm{d}x\mathrm{d}y + \mathcal{O}\left(\frac{|T|}{(\log|T|)^{\sigma/2}}\right).$$

Putting everything together yields

$$\begin{aligned} S(\boldsymbol{v}, j) &= \sum_{n \in I_j} e\left(\operatorname{tr}\left((\widetilde{v_1} + b\widetilde{v_2})\frac{f(z_n)}{b^{j+1}}\right)\right) \\ &= \sum_{\lambda \in r(b^j q)} e\left(\operatorname{tr}\left(\frac{\nu a}{b^j q}\sum_{k=1}^{d} c_k\lambda^k\right)\right)\left\{\iint_{\mathcal{T}} F_\lambda(x,y)\mathrm{d}x\mathrm{d}y + \mathcal{O}\left(\frac{|T|}{(\log|T|)^{\sigma/2}}\right)\right\} \end{aligned}$$

$$= \sum_{\lambda \in r(b^j q)} e\left(\operatorname{tr}\left(\frac{\nu a}{b^j q}\sum_{k=1}^{d} c_k \lambda^k\right)\right) \frac{1}{|b^{j+1}q|^2} \iint_{M_j \le |z|^2 < M} G(z)\mathrm{d}z + \mathcal{O}\left(\frac{X_j}{(\log X_j)^\sigma}\right),$$

where

$$G(z) := e\left(\operatorname{tr}\left(\frac{\hat{v}}{b^{j+1}}\sum_{k=1}^{d} \Omega_k z^k\right)\right).$$

Finally we define rationals $R_i/Q \in \mathbb{Q}(i)$ for $i = 1, \ldots, d$ by

$$\frac{R_i}{Q} = \frac{\hat{v}}{b^j}\frac{ac_i}{q}.$$

Thus estimating the integral trivially and noting that

$$N(\hat{v}Q) = N(b^{j+1}R_i q_i/a_i) \ll\gg N(b^{j+1}R_i\alpha_i^{-1}) \ll\gg N(b^{j+1}R_i) \gg N(b^{j+1})$$

we get by an application of Lemma 4.7

$$S(\boldsymbol{v}, j) = \sum_{n \in I_j} e\left(\operatorname{tr}\left((\widetilde{v_1} + b\widetilde{v_2})\frac{f(z_n)}{b^{j+1}}\right)\right)$$

$$\ll \frac{|b^j q|^2}{N(Q)}(N(Q))^{1-\frac{1}{d}+\varepsilon}\frac{X_j}{|b^j q|^2} + \frac{X_j}{(\log X_j)^\sigma}$$

$$\ll X_j\left((N(\hat{v}^{-1}b^{j+1}))^{-\frac{1}{d}+\varepsilon} + (\log X_j)^{-\sigma}\right). \quad (4.4.28)$$

Plugging this into (4.4.11) yields

$$\left|\sum_{n \in I_j} \mathcal{I}\left(\frac{f(z_n)}{b^{j+1}}\right) - \frac{X_j}{|b|^{2l}}\right| \ll X_j\left(\mu^k\Delta^2 + \frac{2\mu^k}{H+1} + \left(\frac{\mu}{|b|^2}\right)^k + \mu^k\left\{\sum_{\mathbf{0}<\|\boldsymbol{v}\|_\infty \le \Delta^{-1}} + \sum_{\mathbf{0}<\|\boldsymbol{v}\|_\infty \le H}\right\}\right.$$
$$\left.\frac{1}{r(\boldsymbol{v})}\left((N(\hat{v}^{-1}b^{j+1}))^{-\frac{1}{d}+\varepsilon} + (\log X_j)^{-\sigma}\right)\right). \quad (4.4.29)$$

Now we set σ, k, and H with the same values as in (4.4.19) and get together with (4.2.4) that

$$\sigma := G, \quad k := C_k \log\log X_j, \quad H := \mu^k \log X_j, \quad \Delta^{-1} = \frac{(\log X_j)^{C_k \log|b|}}{2c_\Delta},$$

for C_k an arbitrary constant.

We note that

$$|\widetilde{v_1} + b\widetilde{v_2}| = \left|(1, b)(v_1, v_2)^t \Xi^{-1}\right| \ll |(v_1, v_2)| \ll r(\boldsymbol{v}).$$

At this point we have to distinguish two cases according to the size of d.

- $d = 1$: By noting that $\Delta^{-1}, H \ll (\log N)$ we get that

$$\sum_{\mathbf{0}<\|\boldsymbol{v}\|_\infty \le \log N} \frac{1}{r(\boldsymbol{v})}(N(\hat{v}^{-1}b^{j+1}))^{-1+\varepsilon} \ll \sum_{\mathbf{0}<\|\boldsymbol{v}\|_\infty \le \log N} \frac{|\widetilde{v_1} + b\widetilde{v_2}|}{|b|^{(2-\varepsilon)\frac{j+1}{d}}} \ll \frac{(\log N)^4}{|b|^{\frac{2j}{d}}}.$$

- $d \ge 2$: In this case get that

$$r(\boldsymbol{v})^{-1} \ll |\widetilde{v_1} + b\widetilde{v_2}|^{-1} \ll |\widetilde{v_1} + b\widetilde{v_2}|^{-\frac{2}{d}}.$$

This together with $\Delta^{-1}, H \ll \log N$ yields

$$\sum_{\mathbf{0}<\|\boldsymbol{v}\|_\infty \le \log N} \frac{1}{r(\boldsymbol{v})}(N(\hat{v}^{-1}b^{j+1}))^{-\frac{1}{d}+\varepsilon} \ll \sum_{\mathbf{0}<\|\boldsymbol{v}\|_\infty \le \log N} \frac{1}{|b|^{(2-\varepsilon)\frac{j+1}{d}}} \ll \frac{(\log N)^2}{|b|^{\frac{2j}{d}}}.$$

Therefore we get in any case that

$$\sum_{\mathbf{0}<\|\boldsymbol{v}\|_\infty\leq\log N}\frac{1}{r(\boldsymbol{v})}(N(\hat{v}^{-1}b^{j+1}))^{-\frac{1}{d}+\varepsilon}\ll\frac{(\log N)^4}{|b|^{\frac{2j}{d}}}.$$

Putting this all in (4.4.29) yields

$$\left|\sum_{n\in I_j}\mathcal{I}\left(\frac{f(z_n)}{b^{j+1}}\right)-\frac{X_j}{|b|^{2l}}\right|\ll X_j\left((\log X_j)^{-1}+\frac{(\log N)^4\log X_j}{|b|^{\frac{2j}{d}}}\right)\ll\frac{X_j}{j}+X_j\frac{(\log N)^5}{|b|^{\frac{2j}{d}}}. \quad (4.4.30)$$

4.4.6 Putting all together

Now we have reached the final state of the proof. In order to finish we will put (4.4.20), (4.4.24), and (4.4.30) together and consider the corresponding intervals, which are described in (4.4.14), (4.4.15), and (4.4.13), respectively. Thus

$$\sum_{l\leq j\leq J}\left|\sum_{n\in I_j}\mathcal{I}\left(\frac{f(z_n)}{b^{j+1}}\right)-\frac{X_j}{|b|^{2l}}\right|\ll S_1+S_2+S_3, \quad (4.4.31)$$

where

$$S_1=\sum_{l\leq j\leq J}\frac{X_j}{j},$$
$$S_2=\sum_{l\leq j\leq l+C_l\log\log N}X_j\frac{(\log N)^5}{|b|^{\frac{2j}{d}}},$$
$$S_3=\sum_{J-C_u\log\log N\leq j\leq J}\sqrt{X_j}\,|b|^{\frac{j}{d}}+\left(\frac{X_j}{|b|^{\frac{2j}{d}}}\right)^{\frac{\log|b|}{\log C_\mu}}\left(\sqrt{X_j}\,|b|^{\frac{j}{d}}+X_j(\log X_j)^{-3}\right).$$

We estimate each sum and easily get for the first one

$$S_1\ll M.$$

The second one is a bit more delicate and simplifies to

$$S_2\ll\sum_{l\leq j\leq l+C_l\log\log N}M\frac{(\log N)^5}{|b|^{\frac{2j}{d}}}\ll M\frac{(\log N)^5}{|b|^{\frac{2}{d}(C_l\log\log N)}}\ll M,$$

where we have assumed that $C_l\geq 5$. For the third sum we have to do a little more work to get

$$\begin{aligned}S_3&\ll\sum_{J-C_u\log\log N\leq j\leq J}\sqrt{M}\,|b|^{\frac{j}{d}}+\left(\frac{M}{|b|^{\frac{2j}{d}}}\right)^{\frac{\log|b|}{\log C_\mu}}\left(\sqrt{M}\,|b|^{\frac{j}{d}}+M\right)\\&\ll\sqrt{M}\,|b|^{\frac{J}{d}}+\left(\frac{M}{|b|^{\frac{2J}{d}}}\right)^{\frac{\log|b|}{\log C_\mu}}\left(\sqrt{M}\,|b|^{\frac{J}{d}}+M\right)\\&\ll M.\end{aligned}$$

Putting this in (4.4.31) yields

$$\sum_{l\leq j\leq J}\left|\sum_{n\in I_j}\mathcal{I}\left(\frac{f(z_n)}{b^{j+1}}\right)-\frac{X_j}{|b|^{2l}}\right|\ll M\ll\frac{N}{\log N}$$

and the main theorem is proven.

Chapter 5

Weyl Sums in $\mathbb{F}_q[X]$ with digital restrictions

The contents of this chapter is based on a joint work with Thuswaldner [49]. The objective is the study of exponential sums in Laurent series over a finite field $\mathbb{F}_q$. In particular, we are interested in Weyl sums involving terms related to digit representations of elements of the polynomial ring $\mathbb{F}_q[X]$.

5.1 Introduction

Drmota and Gutenbrunner [20] considered exponential sums of the shape

$$\sum_{A\in\mathcal{P}_n} E\left(\sum_{i=1}^{r}\frac{R_i}{M_i}f_i(A)\right) \tag{5.1.1}$$

with $R_i, M_i \in \mathcal{R}$, Q_i-additive functions f_i and an additive character E defined on the field of Laurent series over a finite field (compare (5.2.2) for the exact definition). Estimating such sums they are able to derive results on the structure of subsets of $\mathcal{R}$ that are defined in terms of restrictions of certain Q_i-additive functions. For instance, they show that the values of r quite arbitrary Q_i-additive functions are equidistributed in residue classes with respect to a given element of $\mathcal{R}$. Moreover, they are able to prove normal distribution results involving Q_i-additive functions.

Our aim is to give estimates for exponential sums of a more general structure. In particular, we allow that the argument of the character E in (5.1.1) may contain an additional polynomial summand. This result also forms a generalization of a result of Kubota [46] which is the basis of a treatment of Waring's Problem in function fields. We will dwell on this result again in Section 5.2 after having the necessary notations at hand.

Our exponential sum estimate has several applications. We want to present an equidistribution result for sets of polynomials defined in terms of Q_i-additive functions and a variant of Waring's Problem with digital restrictions in function fields (*cf.* [65] for the integer case of this result). In particular, the present chapter is organized as follows.

- In Section 5.2 we define the basic notions which are standard in this area (*cf.* for instance [8, 12, 17, 18, 33, 46]) and give some preliminary results. Moreover we state the main results of the chapter, *i.e.*, two estimates for Weyl sums in $\mathcal{R}$ with Q_i-additive functions, an equidistribution result and a version of Waring's Problem in $\mathbb{F}_q$ involving restrictions by Q_i-additive functions.

- Section 5.3 is devoted to an estimate for higher auto correlation of Q_i-additive functions. The results of this section are partly generalizations of results of Drmota and Gutenbrunner [20].

- Section 5.15 is devoted to the proof of the Weyl sum estimates. To this matter the correlation result of the previous section is used.
- Sections 5.5 and 5.6 contain the proofs of the uniform distribution results and the version of Waring's Problem in $\mathcal{R}$, respectively.

5.2 Preliminaries and statement of results

We want to state our results on Weyl Sums over the ring $\mathcal{R}$ in this section and review some earlier results related to such sums. To state the results we have to set up a certain additive character which will allow us to define exponential sums. This character will be defined in the field $\mathbb{F}_q((X^{-1}))$ of Laurent series over $\mathbb{F}_q$. $\mathbb{F}_q((X^{-1}))$ will be equipped with the Haar measure. All these objects are standard in this field (see for instance [8, 46]) and we recall their definition briefly.

For $N \in \mathcal{R}$ we denote by $\operatorname{sign} N$ the leading coefficient of N. Then we call a polynomial $P \in \mathcal{R}$ *principal* if its leading coefficient is equal to 1, *i.e.* $\operatorname{sign} P = 1$. In the same manner as above we denote by

$$\mathcal{P}_n := \{A \in \mathcal{R} : \deg A < n\},$$
$$\mathcal{P}'_n := \{A \in \mathcal{R} : A \text{ is principal and } \deg A = n\}$$

the set of polynomials of degree less that n and the set of principal polynomials of degree equal to n, respectively.

We set $\mathcal{K} := \mathbb{F}_q(X)$ for the field of rational polynomials over $\mathbb{F}_q$. Moreover, vectors will be written in boldface, *i.e.*, we will write for instance $\mathbf{D} := (D_1, \dots, D_\ell)$ where ℓ is an integer.

We recall the definition of the valuation ν. Let $A, B \in \mathcal{R}$, then

$$\nu(A/B) := \deg A - \deg B \tag{5.2.1}$$

and $\nu(0) := -\infty$. With help of this valuation we can complete $\mathcal{K}$ to the field $\mathcal{K}_\infty := \mathbb{F}_q((X^{-1}))$ of formal Laurent series. Then we get

$$\nu\left(\sum_{i=-\infty}^{+\infty} a_i X^i\right) = \sup\{i \in \mathbb{Z} : a_i \neq 0\}.$$

Thus for $A \in \mathcal{R}$ we have $\nu(A) = \deg A$.

For convenience if not stated otherwise we will always denote a polynomial in $\mathcal{R}$ by a big Latin letter and a formal Laurent series in $\mathcal{K}_\infty$ by a small Greek letter.

By the definition of $\mathcal{K}_\infty$ we can write every $\alpha \in \mathcal{K}_\infty$ as

$$\alpha = \sum_{k=-\infty}^{\nu(\alpha)} a_k X^k$$

with $a_k \in \mathbb{F}_q$. Then we call $\lfloor \alpha \rfloor := \sum_{k=0}^{\nu(\alpha)} a_k X^k$ the integral part and in the same manner $\{\alpha\} := \alpha - \lfloor \alpha \rfloor$ the fractional part of α. If there exist $A, B \in \mathcal{R}$ such that $\alpha = AB^{-1}$ then we call α *rational*, otherwise α is *irrational*.

Now we define the Haar measure on $\mathcal{K}_\infty$. To this matter we denote by $\mathcal{U}(\ell) := \{A \in \mathcal{K}_\infty : \nu(A) < -\ell\}$. We call $\mathcal{U}_\infty := \mathcal{U}(0)$ the *unit interval*. We normalize the Haar measure on $\mathcal{K}_\infty$ by

$$\int_{\alpha \in \mathcal{U}_\infty} 1 \cdot \mathrm{d}\alpha = 1.$$

Thus we get for all $\beta \in \mathcal{K}_\infty$

$$\int_{\nu(\alpha-\beta)<-n} 1 \cdot \mathrm{d}\alpha = q^{-n}.$$

The next ingredient for the Weyl Sums are additive characters. Let $\alpha \in \mathcal{K}_\infty$, $\alpha = \sum_{i=-\infty}^{\nu(\alpha)} a_i X^i$. Then by $\operatorname{Res}\alpha := a_{-1}$ we denote the residue of an element α. In a finite field $\mathbb{F}_q$ of characteristic $\operatorname{char}\mathbb{F}_q = p$ we define the additive character E by

$$E(\alpha) := \exp\left(2\pi i \operatorname{tr}(\operatorname{Res}\alpha)/p\right), \tag{5.2.2}$$

where $\operatorname{tr} : \mathbb{F}_q \to \mathbb{F}_p$ denotes the usual trace of an element of $\mathbb{F}_q$ in $\mathbb{F}_p$.

This character has the following basic properties which mainly correspond to well-known properties of the character $\exp(2\pi i x)$.

Lemma 5.1 ([46, Lemma 1])**.**

1. *If $\nu(\alpha - \beta) > 1$ then $E(\alpha) = E(\beta)$.*
2. *$E : K_\infty \to \mathbb{C}$ is continuous.*
3. *E is not identically 1.*
4. *$E(\alpha + \beta) = E(\alpha)E(\beta)$.*
5. *$E(A) = 1$ for every $A \in \mathbb{F}_q[X]$.*
6. *For $n \in \mathbb{Z}$ and $N \in \mathcal{R}$ we have*
$$\int_{\nu(\alpha)<-n} E(\alpha N)\mathrm{d}\alpha = \begin{cases} q^{-n} & \text{if } \deg N < n, \\ 0 & \text{otherwise.} \end{cases}$$
7. *For $N, Q \in \mathcal{R}$ we have*
$$\sum_{\deg A < \deg Q} E\left(\frac{A}{Q}N\right) = \begin{cases} q^{\deg Q} & \text{if } Q|N, \\ 0 & \text{otherwise.} \end{cases}$$

The sum in (7) of Lemma 5.1 is a very simple Weyl Sum. We define a general Weyl Sum by

$$S(\alpha, \mathcal{M}, \varphi) := \sum_{A \in \mathcal{M}} E(\alpha\varphi(A)), \tag{5.2.3}$$

where $\alpha \in \mathcal{K}_\infty$, $\mathcal{M} \subset \mathcal{R}$ is a finite set, and $\varphi : \mathcal{R} \to \mathcal{K}_\infty$ is a function.

One of the first results in that area was given by Kubota [46]. It reads as follows

Theorem ([46, Proposition 12])**.** *Let $h(Y) = \alpha Y^k + \alpha_{k-1}Y^{k-1} + \cdots + \alpha_1 Y \in \mathcal{K}_\infty[Y]$ with $k = \deg h < p = \operatorname{char}\mathbb{F}_q$. Suppose that there exist relatively prime polynomials A and Q with $\alpha = \frac{A}{Q} + \beta$ such that $\nu(\beta) \le \nu(Q)^{-2}$ and $n < \nu(Q) \le (k-1)n$. Then*

$$S(\alpha, \mathcal{P}_n, h) \ll q^{n\left(1 - \frac{1}{2^{k-1}} + \varepsilon\right)}. \tag{5.2.4}$$

We denote by $\mathcal{I} \subset \mathcal{R}$ and $\mathcal{I}_n := \mathcal{P}_n \cap \mathcal{I}$ the set of all irreducible polynomials and the set of all irreducible polynomials of degree less than n, respectively. Then Car [8] could prove the following result (see Hayes [33] for the case $k = 1$).

Theorem ([8, Proposition VII.7])**.** *Let $h(Y) = \alpha Y^k + \alpha_{k-1}Y^{k-1} + \cdots + \alpha_1 Y \in \mathcal{K}_\infty[Y]$ with $k = \deg h < p = \operatorname{char}\mathbb{F}_q$. Let*

$$r > 0 \text{ and } n > \sup\left\{4kr, \frac{4qr^2}{(\log q)^2} + 2kr^2\right\}$$

be positive integers. Let H be a polynomial such that $\deg H \in \{2kr, \ldots, kn - 2kr\}$. Then for G a polynomial relatively prime to H

$$S(GH^{-1}, \mathcal{I}_n, h) \ll r(\log n)n^{1+2^{-2-2k}} q^{n-k2^{-2k}r}$$

holds.

In the present chapter we are interested in estimating exponential sums over polynomials that satisfy certain congruences involving Q_i-additive functions. Therefore we recall the definitions of $\mathcal{C}_n(\mathbf{f},\mathbf{J},\mathbf{M})$ and $\mathcal{C}'_n(\mathbf{f},\mathbf{J},\mathbf{M})$.

$$\mathcal{C}_n(\mathbf{f},\mathbf{J},\mathbf{M}) = \mathcal{C}_n(\mathbf{J}) := \{A \in \mathcal{P}_n : f_1(A) \equiv J_1 \bmod M_1, \ldots, f_r(A) \equiv J_r \bmod M_r\},$$
$$\mathcal{C}'_n(\mathbf{f},\mathbf{J},\mathbf{M}) = \mathcal{C}'_n(\mathbf{J}) := \{A \in \mathcal{P}'_n : f_1(A) \equiv J_1 \bmod M_1, \ldots, f_r(A) \equiv J_r \bmod M_r\}.$$

Moreover, let

$$\mathcal{C}(\mathbf{f},\mathbf{J},\mathbf{M}) = \mathcal{C}(\mathbf{J}) := \bigcup_{n\geq 1} \mathcal{C}_n(\mathbf{J}). \tag{5.2.5}$$

Before we state our results we need a numbering of the polynomials in $\mathcal{R}$ and in $\mathcal{C}(\mathbf{J})$. Therefore let τ be a bijection from $\mathbb{F}_q$ into the set $\{0,1,\ldots,q-1\}$ with $\tau(0)=0$. Then we extend τ to $\mathcal{R}$ by setting $\tau(a_kX^k+\cdots+a_1X+a_0) = \tau(a_k)q^k+\cdots+\tau(a_1)q+\tau(a_0)$. Similarly we pull back the relation $\leq$ from $\mathbb{N}$ to $\mathcal{R}$ via τ such that for $A,B\in\mathcal{R}$

$$A \leq B :\Leftrightarrow \tau(A) \leq \tau(B). \tag{5.2.6}$$

By this we get a sequence $\{Z_\ell\}_{\ell\geq 0}$ with $Z_\ell = \tau^{-1}(\ell)$ for all $\ell\in\mathbb{N}$. In the same way we get a sequence $\{W_\ell\}_{\ell\geq 0}$ with $W_\ell \in \mathcal{C}(\mathbf{J})$ for all $\ell\in\mathbb{N}$ and $\tau(W_i)<\tau(W_j) \Leftrightarrow i<j$. Thus $\{Z_\ell\}_{\ell\geq 0}$ and $\{W_\ell\}_{\ell\geq 0}$ are two rising sequences over $\mathcal{R}$ and $\mathcal{C}(\mathbf{J})$ (a sequence $\theta=\{A_\ell\}_{\ell\geq 0}$ of elements in $\mathcal{R}$ is called *rising* if $i<j \Rightarrow \deg A_i \leq \deg A_j$, *cf.* Hodges [35]). Finally we denote by $n_1,n_2,\ldots$ positive integers such that

$$\ell-1 = \deg(W_{n_\ell-1}) < \deg(W_{n_\ell}) = \ell. \tag{5.2.7}$$

With this definition we have that

$$\mathcal{P}_s = \{Z_\ell : 0\leq \ell < q^s\},$$
$$\mathcal{C}_s(\mathbf{J}) = \{W_\ell : 0 \leq \ell < n_s\}.$$

Now we are ready to state our main results. Let φ be a function. Then the difference operator Δ_ℓ ($\ell\geq 0$) is recursively defined by

$$\Delta_0(\varphi(A)) := \varphi(A),$$
$$\Delta_{\ell+1}(\varphi(A);D_1,\ldots,D_{\ell+1}) := \Delta_\ell(\varphi(A+D_{\ell+1});D_1,\ldots,D_\ell) - \Delta_\ell(\varphi(A);D_1,\ldots,D_\ell).$$

Theorem 5.2. *Let $Q_1,\ldots,Q_r\in\mathcal{R}$ be relatively prime with $d_i := \deg Q_i$ be given and for $i\in\{1,\ldots,r\}$ let f_i be a Q_i-additive function. Choose $M_1,\ldots,M_r\in\mathcal{R}$, set $m_i := \deg M_i$, and fix $\mathbf{R}\in\mathcal{P}_{m_1}\times\cdots\times\mathcal{P}_{m_r}$. Let $h(Y)=\alpha_kY^k+\cdots+\alpha_1Y+\alpha_0\in\mathcal{K}_\infty[Y]$ be a polynomial of degree $0<k<\operatorname{char}\mathbb{F}_q$.*

If there exists $\mathbf{H}\in\mathcal{R}^k$ and $A\in\mathcal{R}$ such that

$$E\left(\sum_{i=1}^r \frac{R_i}{M_i}\Delta_k(f_i(A);\mathbf{H})\right) \neq 1,$$

then

$$\sum_{\ell=1}^n E\left(h(Z_\ell)+\sum_{i=1}^r \frac{R_i}{M_i} f_i(Z_\ell)\right) \ll n^{1-2^{-k-1}\gamma} + n^{1-2^{-k-1}\left(\frac{k+5}{2}\right)},$$

where

$$\gamma = 2+\frac{k}{2}+\frac{1-|\Phi_{i,k}(\mathbf{H};d_i)|^2}{dq^{d_i}}$$

with some constant $|\Phi_{i,k}(\mathbf{H};d_i)|\in(0,1)$.

It is easy to deduce the following Corollary.

Corollary 5.3. *Let $Q_1, \dots, Q_r \in \mathcal{R}$ be relatively prime and for $i \in \{1, \dots, r\}$ let f_i be a Q_i-additive function. Choose $M_1, \dots, M_r \in \mathcal{R}$, set $m_i := \deg M_i$, and fix $\mathbf{R} \in \mathcal{P}_{m_1} \times \dots \times \mathcal{P}_{m_r}$. If there exists $\mathbf{H} \in \mathcal{R}^k$ and $A \in \mathcal{R}$ such that*

$$E\left(\sum_{i=1}^{r} \frac{R_i}{M_i} \Delta_k(f_i(A); \mathbf{H})\right) \neq 1,$$

then

$$\sum_{A \in \mathcal{P}_n'} E\left(\alpha\, A^k + \sum_{i=1}^{r} \frac{R_i}{M_i} f_i(A)\right) \ll q^{n\left(1-2^{-k-1}\gamma\right)},$$

where γ is as in Theorem 5.2.

We will use the two results stated above to prove the following theorems. First we use Theorem 5.2 to gain a uniform distribution result.

Theorem 5.4. *Let $Q_1, \dots, Q_r \in \mathcal{R}$ be relatively prime and for $i \in \{1, \dots, r\}$ let f_i be a Q_i-additive function. Choose $M_1, \dots, M_r, J_1, \dots, J_r \in \mathcal{R}$. Let $\{W_i\}_{i \geq 1}$ be the elements of the set $\mathcal{C}(\mathbf{f}, \mathbf{J}, \mathbf{M})$ defined in (5.2.5) ordered by the relation induced by τ in (5.2.6) and $h(Y) = \alpha_k Y^k + \dots + \alpha_1 Y + \alpha_0 \in \mathcal{K}_\infty[Y]$ be a polynomial of degree $0 < k < p = \operatorname{char} \mathbb{F}_q$. Then the sequence $h(W_i)$ is uniformly distributed in $\mathcal{K}_\infty$ if and only if at least one coefficient of $h(Y) - h(0)$ is irrational.*

For the corresponding problem of Waring we say that a polynomial $N \in \mathcal{R}$ is the *strict* sum of k-th powers if it has a representation of the form

$$N = X_1^k + \dots + X_s^k \quad (X_1, \dots, X_s \in \mathcal{R}),$$

where the polynomials $X_1, \dots, X_s$ are each of degree $\leq \lceil \deg N/k \rceil$, *cf.* Definition 1.8 in [24]. Thus the theorem for the strict polynomial Waring reads as follows.

Theorem 5.5. *Let $Q_1, \dots, Q_r \in \mathcal{R}$ be relatively prime and for $i \in \{1, \dots, r\}$ let f_i be a Q_i-additive function. Choose $M_1, \dots, M_r, J_1, \dots, J_r \in \mathcal{R}$ and set $m_i := \deg M_i$. Suppose that for every $\mathbf{0} \neq \mathbf{R} \in \mathcal{P}_{m_1} \times \dots \times \mathcal{P}_{m_r}$ there exists an $A \in \mathcal{R}$ such that*

$$g_0(A) = E\left(\sum_{i=1}^{r} \frac{R_i}{M_i} f_i(A)\right) \neq 1.$$

Let $N \in \mathcal{R}$. If $3 \leq k < p = \operatorname{char} \mathbb{F}_q$ and $n \leq \lceil \deg N/k \rceil$, then for $s \geq k2^k$ and for every N with sufficiently large $\deg N$ we always get a solution for

$$N = \delta_1 P_1^k + \dots + \delta_s P_s^k, \quad (P_i \in \mathcal{C}_n'(\mathbf{f}, \mathbf{J}, \mathbf{M}) \text{ for } i = 1, \dots, s),$$

where $\delta_i \in \mathbb{F}_q$ is a k-th power for $i = 1, \dots, s$ with $\delta_1 + \dots + \delta_s = \operatorname{sign} N$.

5.3 Higher Correlation

The present and the next section are devoted to the proof of Theorem 5.2. Despite some parts of the proof contain similar ideas as the proof of the rational analogue of these results (*cf.* Thuswaldner and Tichy [65, Theorem 3.4]) in our case new phenomena occur and considerable parts of our treatment need other ideas. However, as in the rational case, we use a higher correlation result which is a generalization of a result of Drmota and Gutenbrunner [20, Proposition 3.1]. In particular, [20] contains many of the results of this section for the case $k = 1$ and more specific choices of other parameters.

Recall that $\operatorname{char}\mathbb{F}_q = p$ and that f_i ($1 \le i \le r$) are Q_i-additive functions where $Q_i \in \mathcal{R}$ are pairwise coprime polynomials of degree d_i. Moreover $M_1, \ldots, M_r \in \mathcal{R}$ are polynomials with $m_i := \deg M_i$ for $i = 1, \ldots, r$.

We fix a $\mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}$ and define for $\mathbf{H} \in \mathcal{R}^k$

$$\begin{aligned} g_{\mathbf{R}_i,i,k}(A;\mathbf{H}) = g_{i,k}(A;\mathbf{H}) &:= E\left(\frac{R_i}{M_i}\Delta_k(f_i(A);\mathbf{H})\right), \\ g_{\mathbf{R},k}(A;\mathbf{H}) = g_k(A;\mathbf{H}) &:= \prod_{i=1}^{r} g_{i,k}(A;\mathbf{H}). \end{aligned} \tag{5.3.1}$$

We will omit the $\mathbf{R}$ (resp. the $\mathbf{R}_i$) in the index of g if this omission concerns no confusion.

We define the following correlation functions.

$$\Phi_{i,k}(\mathbf{H};n) := n^{-1}\sum_{\ell=0}^{n-1} g_{i,k}(Z_\ell;\mathbf{H}), \tag{5.3.2}$$

$$\Psi_{i,k}(\mathbf{h};n) := q^{-\sum_{j=1}^{k} h_j} \sum_{H_1\in\mathcal{P}_{h_1}} \cdots \sum_{H_k\in\mathcal{P}_{h_k}} \left|\Phi_{i,k}(\mathbf{H};n)\right|^2. \tag{5.3.3}$$

Furthermore we denote by Φ_k and Ψ_k the corresponding correlations with $g_{i,k}$ replaced by g_k.

Setting

$$\mathcal{P}_n^k := \underbrace{\mathcal{P}_n \times \cdots \times \mathcal{P}_n}_{k \text{ times}}$$

we are in a position to state our correlation result.

Proposition 5.6. *Let $h_1, \ldots, h_k, n$ be positive integers. Let $d = [d_1, \ldots, d_r]$ be the least common multiple of the degrees d_i. Then for every $\mathbf{0} \neq \mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}$ either*

$$\forall A \in \mathcal{R} : g_{\mathbf{R},0}(A) = E\left(\sum_{i=1}^{r}\frac{R_i}{M_i}f_i(A)\right) = 1$$

or there exists an $i \in \{1, \ldots, r\}$ and an $\mathbf{H} \in \mathcal{P}_{d_i}^k$ such that $|\Phi_{i,k}(\mathbf{H};d_i)| < 1$ and

$$\Psi_k(\mathbf{h};n) \ll \exp\left(-\min\left\{h_1,\ldots,h_k,\left\lfloor\frac{\log n}{2\log q}\right\rfloor\right\}\frac{1-|\Phi_{i,k}(\mathbf{H};d_i)|^2}{dq^{d_i}}\right) + n^{-\frac{1}{2}},$$

By taking $h_1 = h_2 = \cdots = h_r$ we get the following specialization.

Corollary 5.7. *Let n be a positive integer. Then for every $\mathbf{0} \neq \mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}$ either*

$$\forall A \in \mathcal{R} : g_{\mathbf{R},0}(A) = E\left(\sum_{i=1}^{r}\frac{R_i}{M_i}f_i(A)\right) = 1$$

or there exists an $i \in \{1, \ldots, r\}$ and an $\mathbf{H} \in \mathcal{P}_{d_i}^k$ such that $|\Phi_{i,k}(\mathbf{H};d_i)| < 1$ and

$$\Psi_k(n,\ldots,n;aq^n) \ll q^{-\eta n}$$

where

$$\eta = \frac{1-\left|\Phi_{i,k}(\mathbf{H};q^{d_i})\right|^2}{d_i q^{d_i}} > 0.$$

In order to show the uniform distribution result mentioned in the introduction we need the following adaption of [20, Proposition 1].

Proposition 5.8. *For every $\mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}$ either*

$$\forall A \in \mathcal{R} : g_{\mathbf{R},0}(A) = E\left(\sum_{i=1}^{r} \frac{R_i}{M_i} f_i(A)\right) = 1$$

or

$$\lim_{n\to\infty} \frac{1}{n} \sum_{\ell=0}^{n-1} g_{\mathbf{R},0}(Z_\ell) = 0$$

holds.

Before we start with the proof we want to take a closer look at $\mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}$ such that $g_{\mathbf{R},0}(A) = 1$ for all $A \in \mathcal{R}$. Let $\mathbf{R}_1$ and $\mathbf{R}_2$ be such that $g_{\mathbf{R}_i,0}(A) = 1$ for $i = 1, 2$. Then

$$\begin{aligned} g_{\mathbf{R}_1+\mathbf{R}_2,0}(A) &= E\left(\sum_{i=1}^{r} \frac{R_{1,i}+R_{2,i}}{M_i} f_i(A)\right) \\ &= E\left(\sum_{i=1}^{r} \frac{R_{1,i}}{M_i} f_i(A) + \sum_{i=1}^{r} \frac{R_{2,i}}{M_i} f_i(A)\right) = g_{\mathbf{R}_1,0}(A) g_{\mathbf{R}_2,0}(A) = 1. \end{aligned}$$

Thus we get that together with the identity element $\mathbf{0}$ that these $\mathbf{R}$ form a group under component wise addition. This group we denote by

$$\mathcal{G} := \{\mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r} : g_{\mathbf{R},0}(A) = 0 \quad \forall A \in \mathcal{R}\}. \tag{5.3.4}$$

In order to prove Propositions 5.6 and 5.8 we start with a very special setting and continue by successively relaxing our prerequisites. Thus the first estimation is for the special case $r = 1$ (see [20, Lemma 3.4] which contains the case $a = 1, k = 1$ of this result).

Lemma 5.9. *Let $h_1, \ldots, h_k, a, n$ be positive integers. Fix $i \in \{1, \ldots, r\}$. If there exists an $\mathbf{H} \in \mathcal{P}_{d_i}^k$ such that $|\Phi_{i,k}(\mathbf{H}; d_i)| < 1$ then*

$$\Psi_{i,k}(\mathbf{h}; aq^n) \ll \exp\left(-\min(h_1, \ldots, h_k, n) \frac{1 - \left|\Phi_{i,k}(\mathbf{H}; q^{d_i})\right|^2}{d_i q^{d_i}}\right).$$

Proof. We fix an $\mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}$. As i and k are fixed throughout the proof of the lemma we set $\Psi := \Psi_{i,k}$, $\Phi := \Phi_{i,k}$, $g := g_{\mathbf{R}?i,i,k}$, $f := f_i$, $d := d_i$.

We can represent every element in $\mathcal{R}$ in Q-ary expansion Thus we define functions $\sigma_0, \sigma_1, \ldots$ iteratively by

$$\begin{aligned} Z_\ell &:= Z_{\sigma_1(\ell)} Q + Z_{\sigma_0(\ell)} \qquad (\deg Z_{\sigma_0(\ell)} < d) \\ \sigma_{t+1}(\ell) &:= \sigma_1(\sigma_t(\ell)). \end{aligned}$$

The following properties of the σ_t are easy to check.

$$\begin{aligned} Z_{\sigma_0(y)} &= Z_y \quad 0 \le y < q^d, \\ Z_{\sigma_t(xq^d+y)} &= Z_{\sigma_t(xq^d)} \quad 0 \le y < q^d, 0 < t, \\ \{Z_{\sigma_t(\ell)} : q^{dt} \le \ell < q^{d(t+1)}\} &= \{Z_\ell : 0 \le \ell < q^d\}. \end{aligned} \tag{5.3.5}$$

Further we define

$$\begin{aligned} \Phi^{(t)}(\mathbf{H}; aq^n) &:= \frac{1}{aq^{n-dt}} \sum_{\ell=0}^{aq^{n-dt}-1} g(Z_{\sigma_t(\ell q^{dt})}; \mathbf{H}), \\ \Psi^{(t)}(\mathbf{h}; aq^n) &:= q^{-\sum_{j=1}^{k} h_j} \sum_{H_1 \in \mathcal{P}_{h_1}} \cdots \sum_{H_k \in \mathcal{P}_{h_k}} \left|\Phi^{(t)}(\mathbf{H}; aq^n)\right|^2 \end{aligned}$$

for $n \geq dt$.

We set

$$s = \frac{\min(h_1, \ldots, h_k, n)}{d} \tag{5.3.6}$$

and show that for $0 \leq t < s$, $P_j \in \mathcal{R}$ and $R_j \in \mathcal{P}_d$ $(j = 1, \ldots, k)$

$$\Phi^{(t)}(\mathbf{P}Q + \mathbf{R}; aq^n) = \Phi^{(t+1)}(\mathbf{P}; aq^n)\Phi(\mathbf{R}; q^d) \tag{5.3.7}$$

holds.

As f is Q-additive we get that $f(P_jQ+R_j) = f(P_j)+f(R_j)$ for $j = 1, \ldots, k$. Further for $A \in \mathcal{R}$ and $I \in \mathcal{P}_d$ we get $g(AQ + I; \mathbf{P}Q + \mathbf{R}) = g(A; \mathbf{P})g(I; \mathbf{R})$. Thus (5.3.5) implies that

$$\begin{aligned}
&aq^{n-dt}\Phi^{(t)}(\mathbf{P}Q + \mathbf{R}; aq^n)\\
&\quad= \sum_{\ell=0}^{aq^{n-dt}-1} g(Z_{\sigma_t(\ell q^{dt})}; \mathbf{P}Q + \mathbf{R})\\
&\quad= \sum_{x=0}^{aq^{n-d(t+1)}-1} \sum_{y=0}^{q^d-1} g(Z_{\sigma_1(\sigma_t(xq^{d(t+1)}+yq^{dt}))}Q + Z_{\sigma_0(\sigma_t(xq^{d(t+1)}+yq^{dt}))}; \mathbf{P}Q + \mathbf{R})\\
&\quad= \sum_{x=0}^{aq^{n-d(t+1)}-1} g(Z_{(\sigma_{t+1}(xq^{d(t+1)}))}; \mathbf{P}) \sum_{y=0}^{q^d-1} g(Z_y; \mathbf{R})\\
&\quad= aq^{n-d(t+1)}\Phi^{(t+1)}(\mathbf{P}; aq^n)q^d\Phi(\mathbf{R}; q^d).
\end{aligned}$$

Now we show that for $\min(h_1, \ldots, h_k) \geq d$

$$\Psi^{(t)}(\mathbf{h}; aq^n) = \Psi^{(t+1)}(\mathbf{h} - d; aq^n)\Psi(d, \ldots, d; q^d),$$

where $\mathbf{h} - d := (h_1 - d, \ldots, h_k - d)$.

Thus, using (5.3.7), we derive

$$\begin{aligned}
&q^{\sum_{j=1}^k h_j}\Psi^{(t)}(\mathbf{h}; aq^n)\\
&\quad= \sum_{P_1\in\mathcal{P}_{h_1-d}} \sum_{R_1\in\mathcal{P}_d} \cdots \sum_{P_k\in\mathcal{P}_{h_k-d}} \sum_{R_k\in\mathcal{P}_d} \overline{\Phi^{(t)}(\mathbf{P}Q + \mathbf{R}; aq^n)}\Phi^{(t)}(\mathbf{P}Q + \mathbf{R}; aq^n)\\
&\quad= \sum_{P_1\in\mathcal{P}_{h_1-d}} \sum_{R_1\in\mathcal{P}_d} \cdots \sum_{P_k\in\mathcal{P}_{h_k-d}} \sum_{R_k\in\mathcal{P}_d} \overline{\Phi^{(t+1)}(\mathbf{P}; aq^n)\Phi(\mathbf{R}; q^d)}\Phi^{(t+1)}(\mathbf{P}; aq^n)\Phi(\mathbf{R}; q^d)\\
&\quad= \sum_{P_1\in\mathcal{P}_{h_1-d}} \cdots \sum_{P_k\in\mathcal{P}_{h_k-d}} \overline{\Phi^{(t+1)}(\mathbf{P}; aq^n)}\Phi^{(t+1)}(\mathbf{P}; aq^n) \sum_{R_1\in\mathcal{P}_d} \cdots \sum_{R_k\in\mathcal{P}_d} \overline{\Phi(\mathbf{R}; q^d)}\Phi(\mathbf{R}; q^d)\\
&\quad= q^{\sum_{j=1}^k h_j - kd}\Psi^{(t+1)}(\mathbf{h} - d; aq^n)q^{kd}\Psi(d, \ldots, d; q^d).
\end{aligned}$$

By the trivial estimation of g we get that $\left|\Psi^{(t)}(\mathbf{h}; n)\right| \leq 1$ for all $\mathbf{h}$, n and t. Furthermore with s as in (5.3.6) we get (note that $\Psi = \Psi^{(0)}$)

$$\Psi(\mathbf{h}; aq^n) = \Psi^{(0)}(\mathbf{h}; aq^n) = \Psi^{(s)}(\mathbf{h} - sd; aq^n)\Psi(d, \ldots, d; q^d)^s.$$

Since $\left|\Psi^{(s)}(\mathbf{h} - sd; aq^n)\right| \leq 1$ this implies that $|\Psi(\mathbf{h}; aq^n)| \leq \left|\Psi(d, \ldots, d; q^d)\right|^s$. Therefore we are left with estimating $\left|\Psi(d, \ldots, d; q^d)\right|$. By hypothesis there exists an $\mathbf{H} \in \mathcal{P}_d^k$ with $\left|\Phi(\mathbf{H}; q^d)\right| < 1$, yielding

$$\Psi(d, \ldots, d; q^d) \leq 1 - \frac{1 - \left|\Phi(\mathbf{H}; q^d)\right|^2}{q^d} \ll \exp\left(-\frac{1 - \left|\Phi(\mathbf{H}; q^d)\right|^2}{q^d}\right).$$

Finally for given $\mathbf{h}$ and n we get that

$$|\Psi(\mathbf{h}; aq^n)| \le \left|\Psi(d, \ldots, d; q^d)\right|^s \ll \exp\left(-\min\left(h_1, \ldots, h_k, n\right) \frac{1 - \left|\Phi(\mathbf{H}; q^d)\right|^2}{dq^d}\right)$$

and the lemma is proven. □

Remark 5.10. As in [20, p.133] we see that $|\Phi_{i,k}(\mathbf{H}; d_i)| = 1$ is uncommon. Indeed, we get

$$\begin{aligned}
&\forall \mathbf{H} \in \mathcal{P}_{d_i}^k : |\Phi_{i,k}(\mathbf{H}; d_i)| = 1 \\
&\quad \Leftrightarrow \forall \mathbf{H} \in \mathcal{P}_{d_i}^k \; \forall A \in \mathcal{P}_{d_i} : g_{i,k}(A; \mathbf{H}) \text{ is constant} \\
&\quad \Leftrightarrow \forall \mathbf{H} \in \mathcal{P}_{d_i}^k \; \forall A, B \in \mathcal{P}_{d_i} : \\
&\quad \overline{g_{i,k-1}(A; \mathbf{H})} g_{i,k-1}(A + H_k; \mathbf{H}) = \overline{g_{i,k-1}(B; \mathbf{H})} g_{i,k-1}(B + H_k; \mathbf{H}) \\
&\quad \Leftrightarrow \forall \mathbf{H} \in \mathcal{P}_{d_i}^{k-1} \; \forall A, B \in \mathcal{P}_{d_i} : g_{i,k-1}(A + B; \mathbf{H}) = g_{i,k-1}(A; \mathbf{H}) g_{i,k-1}(B; \mathbf{H}) \\
&\quad \Leftrightarrow \forall A, B \in \mathcal{P}_{d_i} : g_{i,0}(A + B) = g_{i,0}(A) g_{i,0}(B).
\end{aligned}$$

Thus

$$\begin{gathered}
\exists \mathbf{H} \in \mathcal{P}_d^k : |\Phi_{i,k}(\mathbf{H}; d)| < 1 \\
\Longleftrightarrow \\
\exists A, B \in \mathcal{P}_{d_i} : g_{i,0}(A + B) \ne g_{i,0}(A) g_{i,0}(B).
\end{gathered}$$

Before we generalize Lemma 5.9 to $r > 1$ we need a preliminary lemma.

Lemma 5.11 ([20, Lemma 3.3])**.** *Let f be a completely Q-additive function, and $t \in \mathbb{N}$, $K, R \in \mathcal{R}$ with $\deg R, \deg K < \deg Q^t$. Then for all $N \in \mathcal{R}$ satisfying $N \equiv R \bmod Q^t$ we have*

$$f(N + K) - f(N) = f(R + K) - f(R).$$

Now we are ready for the next step to $r > 1$ (see [20, Lemma 3.5] for a special case of this result).

Lemma 5.12. *Let $k < p$ be a positive integer and $\mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}$ be fixed. If there exist $\mathbf{H} \in \mathcal{P}_{d_i}^k$ such that $|\Phi_{i,k}(\mathbf{H}, d_i)| < 1$ for at least one $i = 1, \ldots, r$ then*

$$\Psi_k(\mathbf{h}; aq^n) \ll \exp\left(-\min\{h_1, \ldots, h_k, n\} \frac{1 - |\Phi_{i,k}(\mathbf{H}; d_i)|^2}{d_i q^{d_i}}\right).$$

Proof. We fix an $\mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}$. Let $\ell \in \{1, \ldots, r\}$ be such that $|\Phi_{\ell,k}(\mathbf{H}, d_\ell)| < 1$. Then we want to reduce the estimation of $\Phi_k(\mathbf{h}; aq^n)$ to the estimation of $\Phi_{\ell,k}(\mathbf{h}; aq^n)$ by trivially estimating the rest. Let $s = \frac{n}{3r}$ and choose t_i ($i \in \{1, \ldots, r\}$) in a way that $b_i = t_i \deg Q_i$ satisfies the inequality $s \le b_i \le 2s$. Now set $B_i = Q_i^{t_i}$ and split the sum over $A \in \mathcal{P}_n$ up according to the congruence classes modulo $B_1, \ldots, B_r$.

Thus for a given $\mathbf{S} \in \mathcal{P}_{b_1} \times \cdots \times \mathcal{P}_{b_r}$ we define

$$N_{\mathbf{S}} := \left\{Z_\ell : 0 \le \ell < aq^n, Z_\ell \equiv S_1 \bmod B_1, \ldots, Z_\ell \equiv S_r \bmod B_r\right\}.$$

For $n \ge \sum_{i=1}^r b_i$ we get by the Chinese Remainder Theorem that

$$|N_{\mathbf{S}}| = \frac{aq^n}{\prod_{i=1}^r q^{b_i}} = aq^{n - \sum_{i=1}^r b_i}.$$

By our choice of the B_j we can apply Lemma 5.11 and get

$$aq^n \Phi_k(\mathbf{H}; n) = \sum_{A \in \mathcal{P}_n} g_k(A; \mathbf{H})$$

$$\begin{aligned}
&= \sum_{\mathbf{S}\in\mathcal{P}_{b_1}\times\cdots\times\mathcal{P}_{b_r}} \sum_{A\in N_{\mathbf{S}}} \prod_{i=1}^{r} g_{i,k}(S_i;\mathbf{H}) \\
&= \sum_{\mathbf{S}\in\mathcal{P}_{b_1}\times\cdots\times\mathcal{P}_{b_r}} \prod_{i=1}^{r} g_{i,k}(S_i;\mathbf{H}) \frac{aq^n}{\prod_{j=1}^{r} q^{b_j}} \\
&= aq^n \prod_{i=1}^{r} q^{-b_i} \sum_{S_i\in\mathcal{P}_{b_i}} g_{i,k}(S_i;\mathbf{H}) \\
&= aq^n \prod_{i=1}^{r} \Phi_{i,k}(\mathbf{H};q^{b_i}).
\end{aligned}$$

Now we take the modulus and estimate $\Phi_{i,k}(\mathbf{H};q^{b_i})$ for $i \neq \ell$ trivially. Thus

$$|\Phi_k(\mathbf{H};aq^n)| \leq \prod_{i=1}^{r} \left|\Phi_{i,k}(\mathbf{H};q^{b_i})\right| \leq \left|\Phi_{\ell,k}(\mathbf{H};q^{b_\ell})\right|.$$

Therefore we can estimate Ψ_k by $\Psi_{\ell,k}$. Noting that $b_\ell \ll n \ll b_\ell$ we get by an application of Lemma 5.9 that

$$\Psi_k(\mathbf{h};aq^n) \leq \Psi_{\ell,k}(\mathbf{h};q^{b_\ell}) \ll \exp\left(-\min\{h_1,\ldots,h_k,n\}\frac{1-\left|\Phi_{\ell,k}(\mathbf{H};q^{d_\ell})\right|^2}{d_\ell q^{d_\ell}}\right).$$

□

Finally we generalize Lemma 5.12 by allowing an arbitrary integer as second argument for Ψ_k.

Lemma 5.13. *Let $k < p$ be a positive integer and $\mathbf{R} \in \mathcal{P}_{m_1}\times\cdots\times\mathcal{P}_{m_r}$ be fixed. Let $d := [d_1,\ldots,d_r]$ be the least multiple. If there exist $\mathbf{H} \in \mathcal{P}_{d_i}^k$ such that $|\Phi_{i,k}(\mathbf{H},d_i)| < 1$ for at least one $i = 1,\ldots r$, then*

$$\Psi_k(\mathbf{h};n) \ll \exp\left(-\min\left\{h_1,\ldots,h_k,\left\lfloor\frac{\log n}{2\log q}\right\rfloor\right\}\frac{1-|\Phi_{i,k}(\mathbf{H};d_i)|^2}{dq^{d_i}}\right).$$

Proof. We fix $\mathbf{R} \in \mathcal{P}_{m_1}\times\cdots\times\mathcal{P}_{m_r}$. As in Lemma 5.12 let ℓ be such that $|\Phi_{\ell,k}(\mathbf{H},d_\ell)| < 1$. Further we set

$$s := \left\lfloor\frac{\log n}{2d\log q}\right\rfloor.$$

First we show how we can split up Φ_k. Define two positive integers a and b with $n = aq^{ds}+b$ and $0 \leq b < q^{ds} \ll n^{\frac{1}{2}}$. Then for any $\mathbf{P} \in \mathcal{R}^k$ and $\mathbf{R} \in \mathcal{P}_{ds}^k$

$$n\Phi_k(\mathbf{P}X^{ds}+\mathbf{R};n) = aq^{ds}\Phi_k(\mathbf{P}X^{ds}+\mathbf{R};aq^{ds}) + c_a(\mathbf{P})b\Phi_k(\mathbf{R};b)$$

holds, where $|c_a(\mathbf{P})| = 1$ is a constant depending on a and $\mathbf{P}$. Indeed, we obtain

$$\begin{aligned}
n\Phi_k(\mathbf{P}X^{ds}+\mathbf{R};n) &= \sum_{\ell=0}^{aq^{ds}-1} g_k(Z_\ell;\mathbf{P}X^{ds}+\mathbf{R}) + \sum_{\ell=aq^{ds}}^{aq^{ds}+b-1} g_k(Z_\ell;\mathbf{P}X^{ds}+\mathbf{R}) \\
&= aq^{ds}\Phi_k(\mathbf{P}X^{ds}+\mathbf{R};aq^{ds}) + \sum_{y=0}^{b-1} g_k(Z_aX^{ds}+Z_y;\mathbf{P}X^{ds}+\mathbf{R}) \\
&= aq^{ds}\Phi_k(\mathbf{P}X^{ds}+\mathbf{R};aq^{ds}) + c_a(\mathbf{P})\,b\Phi_k(\mathbf{R};b).
\end{aligned}$$

Now we show that by skipping the summands corresponding to b we do not lose to much.

$$\left|\Phi_k(\mathbf{P}X^{ds}+\mathbf{R};n) - \Phi_k(\mathbf{P}X^{ds}+\mathbf{R};aq^{ds})\right|$$

$$= \left| \frac{aq^{ds}\Phi_k(\mathbf{P}X^{ds}+\mathbf{R};aq^{ds}) + c_a(\mathbf{P})\, b\Phi_k(\mathbf{R};b)}{n} - \Phi_k(\mathbf{P}X^{ds}+\mathbf{R};aq^{ds}) \right|$$
$$= \frac{b}{n}\left|c_a(\mathbf{P})\Phi_k(\mathbf{R};b) - \Phi_k(\mathbf{P}X^{ds}+\mathbf{R};aq^{ds})\right|$$
$$\ll \frac{b}{n} \ll n^{-\frac{1}{2}}.$$

Thus we get

$$\Phi_k(\mathbf{P}Q^s+\mathbf{R};n) = \Phi_k(\mathbf{P}Q^s+\mathbf{R};aq^{ds}) + \mathcal{O}(n^{-\frac{1}{2}})$$

and, hence,

$$\Psi_k(\mathbf{h};n) = \Psi_k(\mathbf{h};aq^{ds}) + \mathcal{O}(n^{-\frac{1}{2}}).$$

Now we apply Lemma 5.12 to $\Psi_k(\mathbf{h};aq^{ds})$ and get for fixed $\mathbf{h}$

$$\Psi(\mathbf{h};n) \ll \exp\left(-\min\left(h_1,\ldots,h_k,\frac{\log n}{2\log q}\right)\frac{1-\left|\Phi(\mathbf{H};q^{d_\ell})\right|^2}{dq^{d_\ell}}\right) + n^{-\frac{1}{2}}.$$

□

Now we are ready to state the proof of the higher correlation result.

Proof of Proposition 5.6. By the assumptions of Lemma 5.13 we split the proof into two cases.

Case 1: There exist an i and $\mathbf{H} \in \mathcal{P}_d^k$ such that $|\Phi_{i,k}(\mathbf{H};d_i)| < 1$. Then we get the result by an application of Lemma 5.12.

Case 2: If for all i and $\mathbf{H} \in \mathcal{P}_d^k$ we have $|\Phi_{i,k}(\mathbf{H};d_i)| = 1$ then we get by Remark 5.10 that $g_{i,k}(A+B;\mathbf{H}) = g_{i,k}(A;\mathbf{H})g_{i,k}(B;\mathbf{H})$ and consequently

$$g_k(A+B;\mathbf{H}) = g_k(A;\mathbf{H})g_k(B;\mathbf{H}) \tag{5.3.8}$$

for any $A, B \in \mathcal{P}_d$ and thus by the Q_i-additivity of the f_i $(i = 1,\ldots,r)$ also for $A \in \mathcal{R}$. We again distinguish between two cases:

Case 2.1: $g_0(A) = 1$ for every $A \in \mathcal{R}$. This is the first alternative in the proposition.

Case 2.2: There exists $A \in \mathcal{R}$ such that $g_0(A) \neq 1$. In this case the proof is exactly the same as the proof of case 2.2 in [20, p.136]. □

The proof of Corollary 5.7 will follow easily by using Lemma 5.12 instead of Lemma 5.13 in the proof of Proposition 5.6.

Finally we are left to show Proposition 5.8. To this matter we state first the Weyl-van der Corput inequality in $\mathcal{K}_\infty$.

Lemma 5.14 ([18, Lemma 2.1])**.** *Let u be a complex-valued function defined on $\mathcal{R}$. Let n and s be positive integers such that $q^s \leq n$. If $n = aq^s + b$ for a and b positive integers such that $0 \leq b < q^s$, then*

$$q^s(n+q^s-b)^{-1}\left|\sum_{\ell=0}^{n-1} u(Z_\ell)\right|^2 \leq \sum_{P\in\mathcal{P}_s}\sum_{\ell=0}^{n-1}\overline{u(Z_\ell)}u(Z_\ell+P),$$

where $u(B) = 0$ if $\tau(B) \geq 0$.

Proof of Proposition 5.8. We only consider the case that there exists an $\mathbf{R} \in \mathcal{P}_{m_1}\times\cdots\times\mathcal{P}_{m_r}$ with $g_0(A) \neq 1$ as otherwise there is nothing to show. Let s be the greatest integer such that $q^s \leq n$. Let a and b be positive integers such that $n = aq^s + b$ with $0 \leq b < q^s$. Then we apply Lemma 5.14 with $u(A) := g_0(A)$ and get

$$q^s(n+q^s-b)^{-1}\left|\sum_{\ell=0}^{n-1} g_0(Z_\ell)\right|^2 \leq \sum_{P\in\mathcal{P}_s}\sum_{\ell=0}^{n-1}\overline{g_0(Z_\ell)}g_0(Z_\ell+P) = n\sum_{P\in\mathcal{P}_s}\Phi_1(P;n).$$

We apply Cauchy's inequality to get $\Phi_1(n, P)$ squared as follows.

$$q^s(n+q^s-b)^{-2}\left|\sum_{\ell=0}^{n-1} g_0(Z_\ell)\right|^4 \leq n^2 \sum_{P\in\mathcal{P}_s} |\Phi_1(n,P)|^2 = n^2 q^s \Psi_1(s;n),$$

and, hence,

$$\left|\sum_{\ell=0}^{n-1} g_0(Z_\ell)\right|^4 \leq 4n^4\Psi_1(s;n).$$

Now we apply Proposition 5.6 to estimate $\Psi_1(s;n)$ and by noting that $s\to\infty$ with $n\to\infty$ the proposition follows. □

5.4 Weyl's Lemma for Q-additive functions

In this section we prove Theorem 5.2. Therefore we have to estimate sums of the form

$$S_n(\varphi) := \sum_{\ell=0}^{n-1} E(\varphi(Z_\ell)), \tag{5.4.1}$$

where n is a positive integer and φ is a function $\varphi : \mathcal{R}\to\mathcal{K}_\infty$. As we already stated the Weyl-van der Corput inequality in Lemma 5.14, we generalize this result to the case of the kth difference operator.

Lemma 5.15. *Let n and $k < \operatorname{char}\mathbb{F}_q$ be positive integers and u be a complex-valued function defined on $\mathcal{R}$. Let $s_1,\dots,s_k$ be positive integers, such that $q^{s_j}\leq n$ for $j=1,\dots,k$. Further let a_j and b_j be positive integers for $j=1,\dots,k$ such that $n=a_jq^{s_j}+b_j$ and $0\leq b_j<q^{s_j}$. Then*

$$|S_n(\varphi)|^{2^k} \leq \left(\prod_{j=1}^{k}\frac{(n+q^{s_j}-b_j)^{2^{k-j}}}{q^{s_j}}\right)\sum_{P_1\in\mathcal{P}_{s_1}}\cdots\sum_{P_k\in\mathcal{P}_{s_k}}\sum_{\ell=0}^{n-1} E(\Delta_k(\varphi(Z_\ell);P_1,\dots,P_k))$$

holds, where $u(B)=0$ if $\tau(B)\geq n$.

Proof. We show this by induction on k. For $k=1$ this is Lemma 5.14 with $u(Z_\ell) := E(\varphi(Z_\ell))$ for $0\leq\ell<n$.

For $k>1$ we square the induction hypotheses and apply Cauchy's inequality to get

$$\begin{aligned}|S_n(\varphi)|^{2^{k+1}} &\leq \left(\prod_{j=1}^{k}\frac{(n+q^{s_j}-b_j)^{2^{k+1-j}}}{q^{2s_j}}\right)\left|\sum_{P_1\in\mathcal{P}_{s_1}}\cdots\sum_{P_k\in\mathcal{P}_{s_k}}\sum_{\ell=0}^{n-1} E(\Delta_k(\varphi(Z_\ell);P_1,\dots,P_k))\right|^2\\ &\leq \prod_{j=1}^{k}\frac{(n+q^{s_j}-b_j)^{2^{k+1-j}}}{q^{s_j}}\sum_{P_1\in\mathcal{P}_{s_1}}\cdots\sum_{P_k\in\mathcal{P}_{s_k}}\left|\sum_{\ell=0}^{n-1} E(\Delta_k(\varphi(Z_\ell);P_1,\dots,P_k))\right|^2.\end{aligned}$$

Applying Lemma 5.14 with $u(Z_\ell) := E(\Delta_k(\varphi(Z_\ell);P_1,\dots,P_k))$ for the innermost sum yields

$$\begin{aligned}&|S_n(\varphi)|^{2^{k+1}}\\ &\quad\leq \left(\prod_{j=1}^{k+1}\frac{(n+q^{s_j}-b_j)^{2^{k+1-j}}}{q^{s_j}}\right)\sum_{P_1\in\mathcal{P}_{s_1}}\cdots\sum_{P_{k+1}\in\mathcal{P}_{s_{k+1}}}\sum_{\ell=0}^{n-1} E(\Delta_{k+1}(\varphi(Z_\ell);P_1,\dots,P_{k+1})).\end{aligned}$$

Thus the Lemma is proven. □

Now we are ready to prove Theorem 5.2.

Proof of Theorem 5.15. We want to apply our results on higher correlation in Proposition 5.6 together with the generalized Weyl inequality of Lemma 5.13. For the case that we have the exceptional setting described in case 1 of Proposition 5.6, then we will consider the resulting sums in the proofs of Theorem 5.4 and Theorem 5.5 separately.

Before we start we write for short ($h \in \mathcal{K}_\infty[Y]$)

$$S_n(h) := \sum_{\ell=0}^{n-1} E\left(h(Z_\ell) + \sum_{i=1}^{r} \frac{R_i}{M_i} f_i(Z_\ell)\right), \tag{5.4.2}$$

By hypotheses there exists an $1 \le i \le r$ and $\mathbf{H} \in \mathcal{P}_{d_i}^k$ with $|\Phi_{i,k}(\mathbf{H}, d_i)| < 1$.

Let $d = \prod_{i=1}^r d_i$ be the product of the degrees of the Q_i. Then set

$$s := \left\lfloor \frac{\log n}{2d \log q} \right\rfloor.$$

Let a and b be positive integers such that $n = aq^s + b$ and $0 \le b < q^s$. We set

$$\varphi(A) = h(A) + \sum_{i=1}^{r} \frac{R_i}{M_i} f_i(A). \tag{5.4.3}$$

Then an application of Lemma 5.15 with $s_1 = \cdots = s_k = s$ yields

$$|S_n(h)|^{2^k} \le \frac{(n + q^s - b)^{2^k - 1}}{q^{ks}} \sum_{\mathbf{P} \in \mathcal{P}_s^k} \sum_{\ell=0}^{n-1} E(\Delta_k(\varphi(Z_\ell); \mathbf{P}))$$

We have to consider the k-th difference operator of φ. By linearity of the difference operator and (5.4.3) we get

$$\begin{aligned} E(\Delta_k(\varphi(Z_\ell); \mathbf{P})) &= E\left(\Delta_k(h(Z_\ell)) + \Delta_k\left(\sum_{i=1}^{r} \frac{R_i}{M_i} f_i(Z_\ell)\right)\right) \\ &= E\left(k!\alpha_k P_1 \cdots P_k\right) g_k(Z_\ell; \mathbf{P}). \end{aligned}$$

Thus

$$|S_n(\alpha)|^{2^k} \le \frac{(n + q^s - b)^{2^k - 1}}{q^{ks}} \sum_{P_1 \in \mathcal{P}_s} \cdots \sum_{P_k \in \mathcal{P}_s} E\left(k!\alpha_k P_1 \cdots P_k\right) \sum_{\ell=0}^{n-1} g_k(Z_\ell; \mathbf{P}).$$

Taking the modulus and shifting to the innermost sum yields

$$|S_n(h)|^{2^k} \le \frac{(n + q^s - b)^{2^k - 1}}{q^{ks}} \sum_{P_1 \in \mathcal{P}_s} \cdots \sum_{P_k \in \mathcal{P}_s} \left|\sum_{\ell=0}^{n-1} g_k(Z_\ell; \mathbf{P})\right|.$$

We apply Cauchy's inequality to get the modulus squared

$$\begin{aligned} |S_n(h)|^{2^{k+1}} &\le \frac{(n + q^s - b)^{2^{k+1} - 2}}{q^{ks}} \sum_{P_1 \in \mathcal{P}_s} \cdots \sum_{P_k \in \mathcal{P}_s} \left|\sum_{\ell=0}^{n-1} g_k(Z_\ell; \mathbf{P})\right|^2 \\ &= \frac{(n + q^s - b)^{2^{k+1} - 2}}{q^{ks}} \Psi_k(s, \dots, s; n). \end{aligned}$$

Finally we apply Lemma 5.13 to estimate $\Psi_k(s, \dots, s; n)$. Thus

$$|S_n(h)|^{2^{k+1}} \ll \frac{n^{2^{k+1} - 2}}{n^{\frac{k}{2}}} \left(\exp\left(-\left\lfloor \frac{\log n}{2 \log q} \right\rfloor \frac{1 - |\Phi_{i,k}(\mathbf{H}; d_i)|^2}{dq^{d_i}}\right) + n^{-\frac{1}{2}}\right)$$

and therefore

$$S_n(h) \ll n^{1-2^{-k-1}\gamma} + n^{1-2^{-k-1}\left(\frac{k+5}{2}\right)},$$

where

$$\gamma = 2 + \frac{k}{2} + \frac{1 - |\Phi_{i,k}(\mathbf{H}; d_i)|^2}{dq^{d_i}}.$$

□

We can also state the proof of Corollary 5.3.

Proof of Corollary 5.3. This proof will mainly follow with help of Corollary 5.7. We have to rewrite the sum over $\mathcal{P}_n'$ into one over $\mathcal{P}$. We note that $\tau(1) = a \in \{0, 1, \dots, q-1\}$. Thus we get that

$$\begin{aligned}\sum_{A \in \mathcal{P}_n'} E\left(\alpha A^k + \sum_{i=1}^{r} \frac{R_i}{M_i} f_i(A)\right) &= \sum_{\ell = aq^n}^{(a+1)q^n - 1} E\left(\alpha Z_\ell^k + \sum_{i=1}^{r} \frac{R_i}{M_i} f_i(Z_\ell)\right) \\ &\ll \sum_{\ell=0}^{(a+1)q^n - 1} E\left(\alpha Z_\ell^k + \sum_{i=1}^{r} \frac{R_i}{M_i} f_i(Z_\ell)\right).\end{aligned}$$

The rest of the proof runs along the same lines as that of Theorem 5.2, but with Corollary 5.7 applied instead of Proposition 5.6. □

5.5 Uniform Distribution

In this section we want to apply Theorem 5.2 in order to show that sequences of the form $\{h(W_\ell)\}_{\ell \geq 0}$ with $h \in \mathcal{K}_\infty[Y]$ a polynomial are uniformly distributed. Therefore we begin with a definition of uniform distribution in $\mathcal{K}_\infty$. For a general concept of uniform distribution one may consider Kuipers and Niederreiter [47] or Drmota and Tichy [21] for a complete survey on that topic. In this chapter we mainly follow Carlitz [12] and Dijksma [17, 18]. Further investigations on that topic have been done by Car [11] (for k-th roots) and Webb [81] (for an integral form of uniform distribution).

Let $\theta = \{A_i\}_{i \geq 1}$ be a sequence of elements in $\mathcal{K}_\infty$. By $\mathcal{N}_k(N, \beta)$ we denote the number of elements A_i with $1 \leq i \leq N$ and $\deg(A_i - \beta) < -k$. Thus

$$\mathcal{N}_k(N, \beta) := \#\{1 \leq i \leq N : \deg(A_i - \beta) < -k\}.$$

Then we call θ uniformly distributed (according to Carlitz) in $\mathcal{K}_\infty$ if

$$\lim_{N \to \infty} \frac{1}{N} \mathcal{N}_k(N, \beta) = q^{-k} \tag{5.5.1}$$

for all positive integers k and all $\beta \in \mathcal{K}_\infty$.

We are mainly interested in the distribution of the sequences Z_i and W_i defined in Section 5.2.

Now we need the Weyl Criterion for uniformly distributed sequences in $\mathcal{K}_\infty$.

Lemma 5.16 ([12, Theorem 3]). *The sequence $\theta = \{\alpha_i\}_{i \geq 1}$ of elements of $\mathcal{K}_\infty$ is uniformly distributed in $\mathcal{K}_\infty$ if and only if*

$$\lim_{N \to \infty} \frac{1}{N} \sum_{i=1}^{N} E(H\,\alpha_i) = 0$$

for all $0 \neq H \in \mathcal{R}$.

First we need a relation between the number of $W_\ell \leq A$ and the number of $Z_\ell \leq A$. Therefore we define the set

$$\mathcal{J} := \{(f_1(A) \bmod M_1, \ldots, f_r(A) \bmod M_r) : A \in \mathcal{R}\}$$

of all possible congruence classes. Then we expect that the $A \in \mathcal{R}$ are uniformly distributed among these classes. Thus we want to show the following.

Proposition 5.17. *For every* $\mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}$ *we have*

$$\lim_{n\to\infty} \frac{1}{n} \left|\{A \leq Z_{n-1} : f_1(A) \equiv J_1 \bmod M_1, \ldots, f_r(A) \equiv J_r \bmod M_r\}\right| = \frac{1}{|\mathcal{J}|}.$$

In order to prove this we define two additive groups

$$\mathcal{G} := \{\mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r} : \forall A \in \mathcal{R} : \ g_0(A) = 1\}$$

and

$$\mathcal{H}_0 := \left\{\mathbf{S} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r} : \forall \mathbf{R} \in \mathcal{G} : \ E\left(-\sum_{i=1}^r \frac{S_i R_i}{M_i}\right) = 1\right\}.$$

By [20, p.9f] we get that $\mathcal{H} = \mathcal{H}_0$. Further we characterize $\mathcal{H}_0$ by the following function

$$F(\mathbf{S}) := \frac{1}{|\mathcal{G}|} \sum_{\mathbf{R}\in\mathcal{G}} E\left(-\sum_{i=1}^r \frac{S_i R_i}{M_i}\right).$$

This is really a characterization as the following shows.

Lemma 5.18 ([20, Lemma 6])**.** *We have*

$$F(S) = 1 \Leftrightarrow S \in \mathcal{H}_0$$

and

$$F(S) = 0 \Leftrightarrow S \notin \mathcal{H}_0.$$

Furthermore $|\mathcal{G}| \cdot |\mathcal{H}_0| = |\mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}| = q^{\sum_{i=1}^r m_i}$.

Now we can state the proof of Proposition 5.17.

Proof of Proposition 5.17. We get by Proposition 5.8 that

$$\begin{aligned}
&\frac{1}{n} \left|\{A \leq Z_{n-1} : f_1(A) \equiv R_1 \bmod M_1, \ldots, f_r(A) \equiv R_r \bmod M_r\}\right| \\
&= \frac{1}{n} \sum_{\ell=0}^{n-1} q^{-\sum_{i=1}^r m_i} \sum_{\mathbf{R}\in\mathcal{P}_{m_1}\times\cdots\times\mathcal{P}_{m_r}} E\left(\sum_{i=1}^r \frac{R_i}{M_i}(f_i(Z_\ell) - S_i)\right) \\
&= q^{-\sum_{i=1}^r m_i} \sum_{\mathbf{R}\in\mathcal{P}_{m_1}\times\cdots\times\mathcal{P}_{m_r}} \left[E\left(\sum_{i=1}^r -\frac{R_i S_i}{M_i}\right) \frac{1}{n} \sum_{\ell=0}^n g_0(Z_\ell)\right] \\
&= q^{-\sum_{i=1}^r m_i} \sum_{\mathbf{R}\in\mathcal{G}} E\left(\sum_{i=1}^r -\frac{R_i S_i}{M_i}\right) + o(1) \\
&= |\mathcal{G}|\, q^{-\sum_{i=1}^r m_i} F(S) + o(1).
\end{aligned}$$

By an application of Lemma 5.18 the Proposition follows. □

Before we state proof of Theorem 5.4 we need a lemma which provides us with a tool to rewrite a sum over W_ℓ into one over Z_ℓ. Recall that $n_1, n_2, \ldots$ are the quantities defined in (5.2.7).

Lemma 5.19. *Let m be a positive integer and $\varphi : \mathcal{R} \to \mathcal{K}_\infty$ be a function. Then for $n_{s-1} \le m < n_s$ there exists a positive integer n such that $n < q^s$ and*

$$\sum_{\ell=0}^{m-1} E(\varphi(W_\ell)) = \sum_{R_1 \in \mathcal{P}_{m_1}} \cdots \sum_{R_r \in \mathcal{P}_{m_r}} \sum_{\ell=0}^{n-1} E\left(\varphi(Z_\ell) + \sum_{i=1}^{r} \frac{R_i}{M_i}(f_i(Z_\ell) - J_i)\right).$$

Furthermore

$$m \sim \frac{n}{|\mathcal{J}|} \tag{5.5.2}$$

and if $m = n_s$ then $n = q^s$.

Proof. The trick we use to rewrite this sum goes back to Gelfond [25]. We set

$$H_n(\varphi, \mathbf{R}) := \sum_{\ell=0}^{n-1} E\left(\varphi(Z_\ell) + \sum_{i=1}^{r} \frac{R_i}{M_i} f_i(Z_\ell)\right).$$

From this we get for a positive integer m

$$\begin{aligned}
&\sum_{R_1 \in \mathcal{P}_{m_1}} \cdots \sum_{R_r \in \mathcal{P}_{m_r}} E\left(-\sum_{i=1}^{r} \frac{R_i\, J_i}{M_i}\right) H_n(\varphi, \mathbf{R}) \\
&= \sum_{R_1 \in \mathcal{P}_{m_1}} \cdots \sum_{R_r \in \mathcal{P}_{m_r}} \sum_{\ell=0}^{n-1} E\left(\sum_{i=1}^{r} \frac{R_i}{M_i}(f_i(Z_\ell) - J_i)\right) E(\varphi(Z_\ell)) \\
&= q^{\sum_{i=1}^{r} m_i} \sum_{\ell=0}^{m-1} E(\varphi(W_\ell)).
\end{aligned}$$

Finally we are left with estimating m. An application of Proposition 5.17 gives (5.5.2). Whereas the assertion that if $m = n_s$ then $n = q^s$ is trivial. Thus the lemma is proved. □

In order to proof Theorem 5.4 for the case that $g_k(A; \mathbf{H}) = 1$ for all $\mathbf{H} \in \mathcal{R}^k$ and $A \in \mathcal{R}$ we need a Lemma due to Dijksma [17].

Lemma 5.20 ([17, Theorem 2.5])**.** *Let $h(Y) \in \mathcal{K}_\infty[Y]$ be a polynomial of degree k with $0 < k < p = \operatorname{char} \mathbb{F}_q$. Then the sequence $\{f(Z_\ell)\}_{\ell \ge 0}$ is uniformly distributed (mod 1) in $\mathcal{K}_\infty$ if and only if the polynomial $h(Y) - h(0)$ has at least one irrational coefficient.*

After these preparations it is quite easy to show Theorem 5.4.

Proof of Theorem 5.4. We want to use Weyl's Criterion (Lemma 5.16) in order to show uniform distribution. Thus we have to show

$$\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} E(H\, h(W_i)) = 0$$

for every $0 \ne H \in \mathcal{R}$.

To this end we fix an $H \in \mathcal{R}$ and set $\widetilde{h}(Y) := H\, h(Y)$. Furthermore we set

$$S_m(H) := \sum_{\ell=1}^{m-1} E(\widetilde{h}(W_\ell)).$$

First we apply Lemma 5.19 to rewrite the sum. Thus

$$S_m(H) = \sum_{R_1 \in \mathcal{P}_{m_1}} \cdots \sum_{R_r \in \mathcal{P}_{m_r}} \sum_{\ell=0}^{n-1} E\left(\widetilde{h}(Z_\ell) + \sum_{i=1}^{r} \frac{R_i}{M_i}(f_i(Z_\ell) - J_i)\right).$$

We distinguish between the possible cases for $g_{\boldsymbol{R},0}(A)$ for every $\mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}$. We set $\mathcal{G}_1 := \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r} \setminus \mathcal{G}$ where $\mathcal{G}$ is defined in (5.3.4). Thus we get

$$S_m(H) = S_0 + S_1,$$

where

$$S_0 = \sum_{\boldsymbol{R} \in \mathcal{G}} E\left(-\sum_{i=1}^{r} \frac{R_i}{M_i} J_i\right) \sum_{\ell=0}^{n-1} E\left(\widetilde{h}(Z_\ell)\right), \tag{5.5.3}$$

$$S_1 = \sum_{\boldsymbol{R} \in \mathcal{G}_1} \sum_{\ell=0}^{n-1} E\left(\widetilde{h}(Z_\ell) + \sum_{i=1}^{r} \frac{R_i}{M_i}(f_i(Z_\ell) - J_i)\right). \tag{5.5.4}$$

We consider the sums separately and start with S_0. We distinguish two cases according to whether $\mathcal{G} \neq \{\mathbf{0}\}$ or $\mathcal{G} = \{\mathbf{0}\}$. If $\mathcal{G} \neq \{\mathbf{0}\}$, then we get

$$\sum_{\boldsymbol{R} \in \mathcal{G}} E\left(-\sum_{i=1}^{r} \frac{R_i}{M_i} J_i\right) = 0$$

and therefore $S_0 = 0$. On the other hand if $\mathcal{G} = \{\mathbf{0}\}$ we have to consider the sum

$$S_0 = \sum_{\ell=0}^{n-1} E\left(\widetilde{h}(Z_\ell)\right).$$

By hypotheses we have that at least one coefficient of $h(Y) - h(0)$ is irrational. The same holds true for $\tilde{h}(Y) - \tilde{h}(0)$. An application of Lemma 5.20 yields $S_0 = o(n) = o(m)$. Thus we get

$$S_0 = \begin{cases} o(m) & \text{if } |\mathcal{G}| = 1, \\ 0 & \text{otherwise.} \end{cases}$$

For S_1 we apply Theorem 5.2 and get that

$$S_1 = \sum_{\ell=0}^{n-1} E\left(\widetilde{h}(Z_\ell) + \sum_{i=1}^{r} \frac{R_i}{M_i}(f_i(Z_\ell) - J_i)\right) \ll n^{1-2^{-k-1}\gamma} + n^{1-2^{-k-1}\left(\frac{k+5}{2}\right)}.$$

Finally we use (5.5.2) to get

$$S_1 \ll m^{1-2^{-k-1}\gamma} + m^{1-2^{-k-1}\left(\frac{k+5}{2}\right)}.$$

As H was arbitrary we get together with Lemma 5.16 that the sequence is uniformly distributed. □

5.6 Waring's Problem with digital restrictions

In this section we want to treat a version of Waring's Problem in $\mathcal{R}$ with digital restrictions. For convenience we give a brief outline on an earlier result on Waring's Problem in $\mathcal{R}$ by Kubota [46].

Let $\mathcal{A} \subset \mathcal{R}$ and s be a positive integer. We call $\mathcal{A}$ a basis of $\mathcal{R}$ of order s if for every $N \in \mathcal{R}$ there is at least one representation of the form

$$N = P_1 + \cdots + P_s \quad \text{with } P_1, \ldots, P_s \in \mathcal{A}.$$

We call $\mathcal{A}$ an asymptotic basis if this is true for N of sufficiently large degree.

For $\mathcal{A} := \{A^k : A \in \mathcal{R}\}$ the problem corresponds to the classical Waring's Problem and was considered independently by Car [7], Kubota [46] and Webb [82].

For $\mathcal{A} := \{A : A \in \mathcal{R} \text{ and } A \text{ irreducible}\}$, which corresponds to Goldbach's Problem, Hayes [33] considered the number of solutions.

Another variant is the question if it is possible to represent every polynomial N as the sum of two irreducible and a k-power, *i.e.*,

$$N = P_1 + P_2 + A^k \quad P_1, P_2 \text{ irreducible}, A \in \mathcal{R}.$$

This problem was considered by Car in [8].

We want to go one step further and show that for a given $Q_1, \dots, Q_r \in \mathcal{R}$ every sufficiently large N has a representation of the shape

$$N = P_1^k + \cdots + P_s^k \quad \text{with } f_i(P_i) \equiv J_i \pmod{M_i},$$

where f_i is a strictly Q_i-additive function and $J_1, \dots, J_s, M_1, \dots, M_s$ are arbitrary polynomials in $\mathcal{R}$. This result corresponds to one gained recently by Thuswaldner and Tichy in [65] for integers.

Before we state all the results we have gained, we consider the setting in a ring $\mathcal{R}$. We start by stating the strict Problem of Waring in such a ring in the way of Webb [82]. Let $N \in \mathcal{R}$ and k be a positive integer. Then we are looking for the smallest s such that

$$N = \delta_1 P_1^k + \cdots + \delta_s P_s^k, \quad (P_i \in \mathcal{P}'_n \text{ for } 1 \le i \le s), \tag{5.6.1}$$

has a solution for every sufficiently large N. By large we mean that the degree of N should be sufficiently large.

We call $r(N, n, s, k, q)$ the number of solutions of (5.6.1). Then Webb [82] could prove the following result

Proposition 5.21 ([82, Theorem 2])**.** *If $n \le \lceil \deg N/k \rceil$, then for $s \ge k2^k$ we get*

$$r(N, n, s, k, q) = \mathfrak{S} q^{n(s-k)} + \mathcal{O}\left(q^{n(s-k)-n/k}\right).$$

for all N having sufficiently large degree, where $1 \ll \mathfrak{S} \ll 1$.

The proof of this theorem makes use of the circle method and we mainly follow Webb [82].

We adopt this method to the base $\mathcal{A} = \bigcup_n \mathcal{C}'_n(\mathbf{J})$. Thus by $R(N, n, s, k, \mathbf{J}, \mathbf{M}, q)$ we denote the number of solutions of the equation

$$N = \delta_1 P_1^k + \cdots + \delta_s P_s^k, \quad (P_i \in \mathcal{C}'_n(\mathbf{J}) \text{ for } 1 \le i \le s),$$

where $\delta_i \in \mathbb{F}_q$ is a k-th power for $i = 1, \dots, s$ such that $\delta_1 + \cdots + \delta_s = \operatorname{sign} N$.

The rest of this section is devoted to the proof of Theorem 5.5. Here we mainly follow the ideas of Thuswaldner and Tichy in [65].

Proof of Theorem 5.5. Thus we set

$$S_n(\alpha) := \sum_{P \in \mathcal{C}'_n(H)} E(\alpha P^k)$$

and $R(N) := R(N, n, s, k, \mathbf{J}, \mathbf{M}, q)$. Hence,

$$R(N) = \int_{U_\infty} S_n(\delta_1 \alpha) \cdots S_n(\delta_s \alpha) E(-N\alpha) \mathrm{d}\alpha. \tag{5.6.2}$$

To get rid of the set $\mathcal{C}'_n(H)$ we adopt an idea of Gelfond [25], which we already used in Lemma 5.19. Thus we may rewrite $S_n(\alpha)$ as

$$S_n(\alpha) = q^{-m} \sum_{\mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}} \sum_{P \in \mathcal{P}'_n} E\left(\sum_{i=1}^r \frac{R_i}{M_i}(f_i(P) - J_i)\right) E(\alpha P^k).$$

Plugging this into (5.6.2) yields

$$\begin{aligned} R(N) = q^{-ms} \int_{\alpha \in U_\infty} \sum_{P_1 \in \mathcal{P}'_n} \cdots \sum_{P_s \in \mathcal{P}'_n} \sum_{\mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}} \\ \times E\left(\sum_{i=1}^r \frac{R_i}{M_i}(f_i(P_1) - J_i)\right) \cdots E\left(\sum_{i=1}^r \frac{R_i}{M_i}(f_i(P_s) - J_i)\right) \\ \times E(\alpha(P_1^k + \cdots + P_s^k - N)) \mathrm{d}\alpha. \end{aligned}$$

Here we reach the point where it is important to exclude the case that there exists an $\mathbf{0} \neq \mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}$ such that $g_{\mathbf{R},0}(A) = 1$ for all $A \in \mathcal{R}$. Because if $\mathcal{G}$ as defined in (5.3.4) is not the trivial group then we get as in the proof of Theorem 5.4 that

$$\sum_{\boldsymbol{R} \in \mathcal{G}} E\left(-\sum_{i=1}^r \frac{R_i}{M_i} J_i\right) = 0.$$

Thus we have that the main part is zero if $\mathcal{G} \neq \{0\}$. Since by our hypotheses there always exists an $A \in \mathcal{R}$ such that $g_{\mathbf{R},0}(A) \neq 1$ and therefore we get that $\mathcal{G}$ is trivial.

We split the integral up into two parts according to $\mathbf{R}$ and get

$$R(N) = q^{-ms}(I_1 + I_2), \tag{5.6.3}$$

where

$$\begin{aligned} I_1 &= \int_{U_\infty} \sum_{P_1 \in \mathcal{P}'_n} \cdots \sum_{P_s \in \mathcal{P}'_n} E(\alpha(P_1^k + \cdots + P_s^k - N)) \mathrm{d}\alpha, \\ I_2 &= \int_{U_\infty} \sum_{P_1 \in \mathcal{P}'_n} \cdots \sum_{P_s \in \mathcal{P}'_n} \sum_{\mathbf{0} \neq \mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}} \\ &\quad \times E\left(\sum_{i=1}^r \frac{R_i}{M_i}(f_i(P_1) - J_i)\right) \cdots E\left(\sum_{i=1}^r \frac{R_i}{M_i}(f_i(P_s) - J_i)\right) \\ &\quad \times E(\alpha(P_1^k + \cdots + P_s^k - N)) \mathrm{d}\alpha. \end{aligned}$$

Here I_1 corresponds to the integral for Waring's Problem and we apply Proposition 5.21. As we will see I_2 contributes to the error term. From now on we assume that $\mathbf{R} \neq 0$. Then we get

$$I_2 = \sum_{R_1 \in \mathcal{P}_m} \cdots \sum_{R_s \in \mathcal{P}_m} I_{\mathbf{R}}$$

where

$$\begin{aligned} I_{\mathbf{R}} &:= \int_{U_\infty} \prod_{t=1}^s S_{n,t}(\alpha) E(-\alpha N) \mathrm{d}\alpha, \\ S_{n,t}(\alpha) &:= \sum_{P \in \mathcal{P}'_n} E\left(\alpha P^k + \sum_{i=1}^r \frac{R_i}{M_i}(f_i(P) - J_i)\right). \end{aligned}$$

To estimate $I_{\mathbf{R}}$ we split the integral up into two parts according to $s > 2^k$ and get

$$|I_{\mathbf{R}}| \leq \sup_{\alpha,t}(|S_{n,t}(\alpha)|^{s-2^k}) \max_t \left(\int_{\alpha \in U_\infty} |S_{n,t}(\alpha)|^{2^k} \mathrm{d}\alpha\right).$$

For the supremum we apply Corollary 5.3. The integral is estimated by the same trick as by Thuswaldner and Tichy [65]. Noting that

$$\int_{\alpha \in U_\infty} |S_{n,i}(\alpha)|^{2^k} \mathrm{d}\alpha = \sum_{\mathbf{P} \in \mathcal{P}'^{2^k}_n} E\left(\sum_{i=1}^r \frac{R_i}{M_i} \sum_{t=1}^{2^{k-1}} f_i(P_t) - f_i(P_{t+2^{k-1}})\right),$$

where the sum is over all $\mathbf{P} \in {\mathcal{P}'}_n^{2^k}$ such that

$$P_1^k + \cdots + P_{2^{k-1}}^k = P_{2^{k-1}+1}^k + \cdots + P_{2^k}^k.$$

We estimate the sum with the number of solutions of this equation trivially and get

$$\int_{\alpha \in U_\infty} |S_{n,t}(\alpha)|^{2^k} \,\mathrm{d}\alpha \ll \int_{\alpha \in U_\infty} \left| \sum_{P \in \mathcal{P}'_n} E(\alpha P^k) \right|^{2^k} \mathrm{d}\alpha. \tag{5.6.4}$$

For the last integral we need the Lemma of Hua in $\mathcal{K}_\infty$.

Lemma 5.22 (*cf.* Theorem 8.13 in [24]). *Let $F(Y)$ be a polynomial over $\mathcal{R}$ and let ν be an integer such that $\Delta_\nu(F(Y); Y_1, \ldots, Y_\nu) \in \mathcal{R}[Y, Y_1, \ldots, Y_\nu]$ and*

$$\Delta_\nu(F(Y); Y_1, \ldots, Y_\nu) \neq 0.$$

Then, for every $\varepsilon > 0$,

$$\int_{\alpha \in U_\infty} \left| \sum_{P \in \mathcal{P}'_\ell} E(\alpha F(P)) \right|^{2^\nu} \mathrm{d}\alpha \ll q^{\ell(2^\nu - \nu + \varepsilon)}.$$

We apply this lemma in (5.6.4) and get

$$\int_{\alpha \in U_\infty} |S_{n,i}(\alpha)|^{2^k} \,\mathrm{d}\alpha \ll q^{n(2^k - k + \varepsilon)}.$$

Together with Corollary 5.3 for the supremum this yields for I_2

$$I_2 \ll q^{n(1-2^{-k-1}-\gamma)(s-2^k)} \, q^{n(2^k-k+\varepsilon)} \ll q^{n(s-k)-n/k}$$

where γ is as in Theorem 5.2.

As this is smaller than the main part in Proposition 5.21, this corresponds to the error term and Theorem 5.5 is proven. □

Remark 5.23. We can further generalize Theorem 5.4 such that every P_t for $t = 1, \ldots, s$ has its own congruence set $\mathcal{C}_{n,t}(\mathbf{f}_t, \mathbf{J}_t, \mathbf{M}_t)$. This goes down the same lines but with tedious index notation.

Since if $\mathcal{G} \neq \{0\}$ we only get that $M_i \mid R_i f_i(A)$ for all $A \in \mathcal{R}$, one has to rewrite the main part in Waring's problem in order to get rid of the assumption $g_0(A) \neq 1$.

Chapter 6

Weyl Sums in $\mathbb{F}_q[X, Y]$ with digital restrictions

In this chapter we want to generalize the results of the preceding one to the function field $\mathbb{F}_q(X,Y)/p(X,Y)\mathbb{F}_q(X,Y)$ where $p(X,Y)$ is a polynomial. This is based on joint work with Thuswaldner [48].

6.1 Preliminaries and definitions

We look that the field $\mathbb{F}_q(X,Y)/p(X,Y)\mathbb{F}_q(X,Y)$ as a finite separable extension of $\mathbb{F}_q(X)$. We will use the following short hand notation where we mainly follow those in [10] and [83]. Let $\mathbb{K} = \mathbb{F}_q(X)$ be the field of rational polynomials over a finite fields and $\mathbb{K}_\infty = \mathbb{F}_q((X^{-1}))$ its completion for the valuation at ∞, *i.e.* for every $\alpha = \frac{A}{B} \in \mathbb{K}$ let

$$\nu(\alpha) = \nu_\infty(\alpha) := \deg B - \deg A$$

be the valuation at ∞ (the inverse degree valuation). Let $\mathbb{L} = \mathbb{F}_q(X,Y)/p(X,Y)\mathbb{F}_q(X,Y)$ be an extension of degree n of $\mathbb{K}_\infty$ where $p(X,Y)$ is a separable polynomial. We write $n = e \cdot f$ where e is the ramification index and f the residue class degree. By $\mathbb{A} = \mathbb{F}_q[X]$ we denote the ring of integers of $\mathbb{K}$ and by $\mathbb{B} = \mathbb{F}_q[X,Y]/p(X,Y)\mathbb{F}_q[X,Y]$ the integral closure of $\mathbb{A}$ in $\mathbb{L}$. Let $\mathfrak{D}$ be the different of the extension $\mathbb{B}$ of $\mathbb{A}$ and let D be the monic polynomial in $\mathbb{A}$ such that the principal ideal $\mathbb{A}D$ is the discriminant of the extension. Finally we denote by ω the extension of ν to $\mathbb{L}$ and by $\mathbb{L}_\infty$ the completion of $\mathbb{L}$ for ω.

In order to get an extension of the degree in $\mathbb{B}$ we put for every $\alpha \in \mathbb{L}_\infty$,

$$d(\alpha) := -\omega(\alpha). \tag{6.1.1}$$

It is clear by the definition of d that $d(A) = \deg(A)$ for every $A \in \mathbb{A}$. Furthermore by the Theorem of Puiseux (*cf.* Theorem 4.1.1 of [14]) we get that there exists $a, b \in \mathbb{N}$ such that

$$d(Y) = \frac{a}{b}.$$

For any non-zero fractional ideal J of $\mathbb{L}$ we denote by $\mathsf{J}(m)$ the set of all $J \in \mathsf{J}$ such that $d(J) \leq m$. Thus especially for $\mathbb{B}$ we get that

$$\mathbb{B}(m) := \{A \in \mathbb{B} : d(A) \leq m\}.$$

Let g be the genus of $\mathbb{L}$ then we get by Equation (I.2.6) of [10] that for $m \cdot f > 2g - 2$

$$\#\mathbb{B}(m) = q^{1-g+mf}. \tag{6.1.2}$$

Let I and J be two non-zero fractional ideals of $\mathbb{L}$ such that $I \subset \mathsf{J}$. Furthermore let $\mathcal{I}$ and $\mathcal{J}$ be any part of J. Then the property "$\mathcal{I}$ is a complete set of representatives of congruence classes modulo I in $\mathcal{I}$" will be denoted by $\mathcal{I} \cong \mathcal{J}/\mathsf{I}$ (*cf.* p.5 of [10]).

As we are mainly interested in properties of number systems in these fields we remind the reader of the definitions in chapter 1. Let $(p(X,Y),\mathcal{D})$ be a number system in $\mathbb{L}$ and $d := \deg p_0$ the degree of the constant part of p when written as a polynomial in Y, *i.e.*,

$$p(X,Y) = Y^n + p_{n-1}Y^{n-1} + \cdots + p_1 Y + p_0 \quad (p_0,\dots,p_{n-1} \in \mathbb{A}).$$

By $\mathcal{L}_m$ we denote all $Q \in \mathbb{B}$ whose length is less than m, *i.e.*

$$\mathcal{L}_m := \{Q \in \mathbb{B} \mid L(Q) < m\}$$

The objective of this chapter will be so called Y-additive functions on $\mathbb{B}$. We call a function $f : \mathbb{B} \to G$, where G is a group, strongly Y-additive if $f(AY + B) = f(A) + f(B)$. Thus, if we represent an element $Q \in \mathbb{B}$ by its Y-ary digital expansion (1.2.4), we may write

$$f(Q) = \sum_{i \geq 0} f(D_i).$$

One simple example is the *sum of digits function*, which is defined by

$$s_Y(Q) := \sum_{i \geq 0} D_i.$$

Throughout the rest of the chapter we fix a Y-additive function f.

In this chapter we mainly investigate Weyl sums with digital restrictions. Therefore we need additive characters. Let $\operatorname{tr}(\alpha)$ be the trace of an element in $\mathbb{L}_\infty$ over $\mathbb{K}_\infty$ and Res be the residuum of an element of $\mathbb{A}$, *i.e.*,

$$\operatorname{Res}\left(\sum_{j \in \mathbb{Z}} a_j X^j\right) = a_{-1}.$$

Furthermore let ψ be a non-principal character on $\mathbb{F}_q$. Then we define a character E on $\mathbb{L}_\infty$ by

$$E(x) := \psi\left(\operatorname{Res} \circ \operatorname{tr}(x)\right). \tag{6.1.3}$$

Now we state our first result which estimates a certain Weyl sum which we will use in order to solve Waring's Problem.

Theorem 6.1. *Let $h \in \mathbb{L}_\infty[Z]$ be a polynomial of degree $k < \operatorname{char} \mathbb{L}$ and f be a Y-additive function. Furthermore let $M \in \mathbb{B}$ and $0 \neq R \in \mathcal{D}^{-1}$. If there exists $\mathbf{H} \in \mathcal{L}_b^k$ such that*

$$\left|\sum_{A \in \mathcal{L}_b} E\left(\frac{R}{M}\Delta_k(f(A);\mathbf{H})\right)\right| < q^{db},$$

then

$$\sum_{A \in \mathbb{B}(n)} E\left(h(A) + \frac{R}{M} f(A)\right) \ll (\#\mathbb{B}(n))^{1-\frac{k+2}{2^{k+1}}} \exp\left(-2^{-(k+1)}\frac{n}{a}\frac{1 - |\Lambda(\mathbf{H})|^2}{q^{db}}\right)$$

For the corresponding Waring's Problem we say that a polynomial $N \in \mathbb{B}$ is the *strict* sum of k-th powers if it has a representation of the form

$$N = X_1^k + \cdots + X_s^k \quad (X_1,\dots,X_s \in \mathbb{B}(m)),$$

where m is such that

$$k(m-1) < d(N) \leq km.$$

Theorem 6.2. *Let f be a Y-additive function. Choose $M \in \mathbb{B}$ and $J \in \mathcal{M} \cong \mathbb{B}/\mathbb{B}M$. Suppose that for every $R \in \mathcal{M}$ there exists an $H \in \mathcal{L}_b$ such that*

$$\left| \sum_{A \in \mathcal{L}_b} E\left(\frac{R}{M}\Delta_k(f(A);\mathbf{H})\right)\right| < q^{db}.$$

Let s be an integer such that $s > 2^k$. Then every $N \in \mathbb{B}$, such that $\deg(\mathrm{N}(N))$ *is sufficiently large, admits a representation as strict sum of k-th powers of the form*

$$N = P_1^k + \cdots + P_s^k \quad \text{with } P_i \in \mathbb{B}(m) \text{ and } f(P_i) \equiv J \pmod{M}$$

6.2 Higher Correlation

Before we start proving our higher correlation result we have to consider the relation between the sets $\mathbb{B}(n)$ and $\mathcal{L}(m)$. As mentioned above there exist $a, b \in \mathbb{N}$ such that $d(Y) = \frac{a}{b}$. Thus we get for $A_0, \ldots, A_m \in \mathcal{N}$ that

$$d(A_mY^m + \cdots + A_1Y + A_0) = \max(\deg(A_m) + m\tfrac{a}{b}, \ldots, \det(A_1) + 1\tfrac{a}{b}, \deg(A_0)).$$

Therefore we can write

$$\mathbb{B}(n) = \left\{A_mY^m + \cdots + A_1Y + A_0 \mid \max_{i=1}^{m}(\deg(A_i) + i\tfrac{a}{b}) \le n\right\}.$$

Let $d := \deg p_0$. We split this set up into smaller parts $\mathbb{B}(n,r)$ for $r = 1, \ldots, d$ as follows.

$$\mathbb{B}(n,0) := \emptyset,$$
$$\mathbb{B}(n,r) := \left\{A_mY^m + \cdots + A_0 \middle| \substack{m \le \frac{b}{a}(n-(d-r)),\\ 1\le j\le r: 0 \le i \le m-(r-j)\frac{b}{a}: \deg A_i \le d-j}\right\} \setminus \mathbb{B}(n,r-1).$$

As one easily checks we get that

$$\mathbb{B}(n) = \bigcup_{r=1}^{d} \mathbb{B}(n,r).$$

Now we assume that $n \ge (d-1)\cdot b + a$ and fix an $1 \le r \le d$. Every $A \in \mathbb{B}(n,r)$ can be written uniquely as $A = PY^b + R$ with P and $R \in \mathbb{B}$. Furthermore one easily checks that $P \in \mathbb{B}(n-a,r)$ and $R \in \mathcal{L}_b$. Thus we get

$$\mathbb{B}(n) = \left\{PY^b + R \mid P \in \mathbb{B}(n-a), R \in \mathcal{L}_b\right\}.$$

Recall that $\operatorname{char}\mathbb{F}_q = p$ and that f is a Y-additive function, moreover let $M \in \mathbb{B}$ be a polynomial. For $k \ge 0$ we recursively define the k-times difference function Δ_k by

$$\Delta_0(f(A)) = f(A),$$
$$\Delta_{k+1}(f(A); H_1, \ldots, H_{k+1}) = \Delta_k(f(A+H_{k+1}); H_1, \ldots, H_k) - \Delta_k(f(A); H_1, \ldots, H_k)$$

Throughout the rest of this section let M be as in Theorem 6.1 and $\mathcal{M} \cong \mathbb{B}/\mathbb{B}M$. We define for $R \in \mathcal{M}$ and $\mathbf{H} \in \mathbb{B}^k$

$$g_{R,k}(A;\mathbf{H}) = g_k(A;\mathbf{H}) := E\left(\frac{R}{M}\Delta_k(f(A);\mathbf{H})\right). \tag{6.2.1}$$

We will omit the R in the index of g if there will be no confusion.

In order to show our correlation results we define the following functions.

$$\Phi_k(\mathbf{H};n) := \frac{1}{\#\mathbb{B}(n)} \sum_{A \in \mathbb{B}(n)} g_k(A;\mathbf{H}), \tag{6.2.2}$$

$$\Psi_k(\mathbf{h};n) := \prod_{i=1}^{k} (\#\mathbb{B}(h_i))^{-1} \sum_{H_1\in\mathbb{B}(h_1)} \cdots \sum_{H_k\in\mathbb{B}(h_k)} |\Phi_k(\mathbf{H};n)|^2, \tag{6.2.3}$$

$$\Lambda_k(\mathbf{H}) := q^{-db} \sum_{A\in\mathcal{L}_b} g_k(A;\mathbf{H}). \tag{6.2.4}$$

We are now in a position to state our correlation result.

Proposition 6.3. *Let $h_1,\dots,h_k,n$ be positive integers. Then for every $0 \neq R \in \mathcal{M} \cong \mathbb{B}/\mathbb{B}M$ either*

$$\forall A \in \mathbb{B} : g_{R,0}(A) = E\left(\frac{R}{M} f(A)\right) = 1$$

or there exists an $\mathbf{H} \in \mathcal{L}_b^k$ such that $|\Lambda_k(\mathbf{H})| < 1$ and

$$\Psi(\mathbf{h};n) \ll \exp\left(-\min(h_1,\dots,h_k,n)\,\frac{1-|\Lambda(\mathbf{H})|^2}{aq^{db}}\right).$$

Before we start with the proof we want to take a closer look at those $R \in \mathcal{M} \cong \mathbb{B}/\mathbb{B}M$ such that $g_{R,0}(A) = 1$ for all $A \in \mathbb{B}$. Let R_1 and $R_2 \in \mathcal{M}$ be such that $g_{R_1,0}(A) = g_{R_2,0}(A) = 1$. Then

$$g_{R_1+R_2,0}(A) = E\left(\frac{R_1+R_2}{M} f(A)\right) = E\left(\frac{R_1}{M} f(A) + \frac{R_2}{M} f(A)\right) = g_{R_1,0}(A) g_{R_2,0}(A) = 1.$$

Thus we get that together with the identity element 0 these R form a group under component wise addition (*cf.* 5.3.4). This group we denote by

$$\mathcal{G} := \{R \in \mathbb{B}/M\mathbb{B} : g_{R,0}(A) = 0 \quad \forall A \in \mathbb{B}\}. \tag{6.2.5}$$

Lemma 6.4. *Let $k < p$ be a positive integer and $R \in \mathcal{M} \cong \mathbb{B}/\mathbb{B}M$ be fixed. If there exists $\mathbf{H} \in \mathcal{L}_a^k$ such that $|\Lambda_k(\mathbf{H})| < 1$, then*

$$\Psi_k(\mathbf{h};n) \ll \exp\left(-\min(h_1,\dots,h_k,n)\,\frac{1-|\Lambda_k(\mathbf{H})|^2}{aq^{db}}\right).$$

Proof. We fix an $R \in \mathcal{M} \cong \mathbb{B}/\mathbb{B}M$. As k is fixed throughout the proof we set $\Psi := \Psi_k$, $\Phi := \Phi_k$, $\Lambda_k := \Lambda$, $g := g_{R,k}$, $f := f$, $d := d_i$.

Since $(p(X,Y),\mathcal{D})$ is a number system we can represent every element $A \in \mathbb{B}$ with $L(A) \geq b$ uniquely as $A = PY^b + R$ where $L(R) < b$, we show that

$$\Phi(\mathbf{P}Y^b + \mathbf{R};n) = \Phi(\mathbf{P};n-a)\Lambda(\mathbf{R}) \tag{6.2.6}$$

holds.

$$\begin{aligned}
(\#\mathbb{B}(n))\Phi(\mathbf{P}Y^b + \mathbf{R};n) &= \sum_{A\in\mathbb{B}(n)} g(A;\mathbf{P}Y^b+\mathbf{R}) \\
&= \sum_{B\in\mathbb{B}(n-a)} \sum_{L\in\mathcal{L}_a} g(BY^b + L;\mathbf{P}Y^b+\mathbf{R}) \\
&= \sum_{B\in\mathbb{B}(n-a)} g(B;\mathbf{P}) \sum_{L\in L_a} g(L;\mathbf{R}) \\
&= (\#\mathbb{B}(n-a))\Phi(\mathbf{P};n-a)\, q^{db}\Lambda(\mathbf{R})
\end{aligned}$$

We set

$$\Xi := q^{-kdb} \sum_{L_1\in\mathcal{L}_b} \cdots \sum_{L_k\in\mathcal{L}_b} |\Lambda(\mathbf{L})|^2. \tag{6.2.7}$$

Now we show that for $\min(h_1,\dots,h_k) \geq a$

$$\Psi(\mathbf{h};n) = \Psi(\mathbf{h}-a;n-a)\Xi,$$

where $\mathbf{h}-a := (h_1-a,\dots,h_k-a)$.

Thus we derive

$$\begin{aligned}
&\prod_{j=1}^{k} (\#\mathbb{B}(h_j))\,\Psi(\mathbf{h};n)\\
&\quad= \sum_{P_1\in\mathbb{B}(h_1-a)}\sum_{R_1\in\mathcal{L}_b}\cdots\sum_{P_k\in\mathbb{B}(h_k-a)}\sum_{R_k\in\mathcal{L}_b}\overline{\Phi(\mathbf{P}Y^b+\mathbf{R};n)}\Phi(\mathbf{P}Y^b+\mathbf{R};n)\\
&\quad= \sum_{P_1\in\mathbb{B}(h_1-a)}\sum_{R_1\in\mathcal{L}_b}\cdots\sum_{P_k\in\mathbb{B}(h_k-a)}\sum_{R_k\in\mathcal{L}_b}\overline{\Phi(\mathbf{P};n-a)\Lambda(\mathbf{R})}\Phi(\mathbf{P};n-a)\Lambda(\mathbf{R})\\
&\quad= \sum_{P_1\mathbb{B}(h_1-a)}\cdots\sum_{P_k\in\mathbb{B}(h_k-a)}\overline{\Phi(\mathbf{P};n-a)}\Phi(\mathbf{P};n-1)\sum_{R_1\in\mathcal{L}_b}\cdots\sum_{R_k\in\mathcal{L}_b}\overline{\Lambda(\mathbf{R})}\Lambda(\mathbf{R})\\
&\quad= \prod_{j=1}^{k}(\#\mathbb{B}(h_j-a))\,\Psi(\mathbf{h}-a;n-a)\,q^{kdb}\Xi.
\end{aligned}$$

By the trivial estimation of g we get that $|\Psi(\mathbf{h};n)| \leq 1$ for all $\mathbf{h}$ and n. Furthermore for $s \leq \min(h_1,\dots,h_k,n)/a$ we get

$$\Psi(\mathbf{h};n) = \Psi(\mathbf{h}-sa;n-sa)\,\Xi^s.$$

Since $|\Psi(\mathbf{h}-sa;n-sa)| \leq 1$ this implies that $|\Psi(\mathbf{h}-sa;n-sa)| \leq |\Xi|^s$. Therefore we are left with estimating $|\Xi|$. By hypothesis there exists an $\mathbf{H}\in\mathcal{L}_b^k$ with $|\Lambda(\mathbf{H})|<1$, yielding

$$\Xi \leq 1 - \frac{1-|\Lambda(\mathbf{H})|^2}{q^{db}} \ll \exp\left(-\frac{1-|\Lambda(\mathbf{H})|^2}{q^{db}}\right).$$

Finally for given $\mathbf{h}$ and n we get that

$$|\Psi(\mathbf{h};n)| \leq |\Xi|^s \ll \exp\left(-\min(h_1,\dots,h_k,n)\,\frac{1-|\Lambda(\mathbf{H})|^2}{aq^{db}}\right)$$

and the lemma is proven. □

Now we consider the Remark of Lemma 3.4 of Drmota and Gutenbrunner [20] and Remark 5.10 in order to show that $|\Lambda_k(\mathbf{H})| = 1$ is uncommon.

Remark 6.5. $|\Lambda_k(\mathbf{H})| = 1$ is uncommon. Indeed, we get

$$\begin{aligned}
&\forall\mathbf{H}\in\mathcal{L}_a^k : |\Lambda_k(\mathbf{H})| = 1\\
&\quad\Leftrightarrow \forall\mathbf{H}\in\mathcal{L}_a^k\,\forall A\in\mathcal{L}_b : g_k(A;\mathbf{H}) \text{ is constant}\\
&\quad\Leftrightarrow \forall\mathbf{H}\in\mathcal{L}_a^k\,\forall A,B\in\mathcal{L}_b :\\
&\quad\overline{g_{k-1}(A;\mathbf{H})}g_{k-1}(A+H_k;\mathbf{H}) = \overline{g_{k-1}(B;\mathbf{H})}g_{k-1}(B+H_k;\mathbf{H})\\
&\quad\Leftrightarrow \forall\mathbf{H}\in\mathcal{L}_a^{k-1}\,\forall A,B\in\mathcal{L}_b : g_{k-1}(A+B;\mathbf{H}) = g_{k-1}(A;\mathbf{H})g_{k-1}(B;\mathbf{H})\\
&\quad\Leftrightarrow \forall A,B\in\mathcal{L}_b : g_0(A+B) = g_0(A)g_0(B).
\end{aligned}$$

Thus

$$\begin{gathered}
\exists\mathbf{H}\in\mathcal{L}_a^k : |\Lambda_k(\mathbf{H})| < 1\\
\Longleftrightarrow\\
\exists A,B\in\mathcal{L}_b : g_0(A+B) \neq g_0(A)g_0(B).
\end{gathered}$$

Now we are ready to state the proof of the higher correlation result.

Proof of Proposition 6.3. By the assumptions of Lemma 6.4 we split the proof into two cases.

Case 1: There exist an $\mathbf{H} \in \mathcal{L}_b^k$ such that $|\Lambda_k(\mathbf{H})| < 1$. Then we get the result by an application of Lemma 6.4.

Case 2: If for all $\mathbf{H} \in \mathcal{L}_b^k$ we have $|\Lambda_k(\mathbf{H})| = 1$ then we get by Remark 6.5 that

$$g_k(A+B;\mathbf{H}) = g_k(A;\mathbf{H})g_k(B;\mathbf{H}) \tag{6.2.8}$$

for any $A, B \in \mathcal{L}_b$ and thus by the Y-additivity of f also for $A \in \mathbb{B}$. We again distinguish between two cases:

Case 2.1: $g_0(A) = 1$ for every $A \in \mathbb{B}$. This is the first alternative in the proposition.

Case 2.2: There exists an $A \in \mathbb{B}$ such that $g_0(A) \neq 1$. In this case the proof is exactly the same as the proof of case 2.2 in [20, p.136]. ☐

6.3 Weyl's Lemma

In this section we prove Theorem 6.1. Therefore we have to estimate sums of the form

$$S_n(\varphi) := \sum_{\ell=0}^{n-1} E(\varphi(Z_\ell)), \tag{6.3.1}$$

We want to apply our results on higher correlation in Proposition 6.3 together with the generalized Weyl inequality.

Our aim is to estimate ($h \in \mathbb{L}_\infty[Z]$)

$$\sum_{A\in\mathbb{B}(n)} E\left(h(A) + \frac{R}{M}f(A)\right),$$

By hypotheses there exists an $\mathbf{H} \in \mathcal{L}_a^k$ with $|\Lambda_k(\mathbf{H})| < 1$. We set

$$s := \left\lfloor \frac{n}{a} \right\rfloor.$$

Let u and v be positive integers such that $n = uq^{ds} + v$ and $0 \le v < q^{ds}$. We further set

$$\varphi(A) = h(A) + \frac{R}{M}f(A). \tag{6.3.2}$$

Then we apply Weyl's method to get the following estimation.

$$|S_n(h)|^{2^k} \le (\#\mathbb{B}(n))^{2^k-k-1} \sum_{P_1\in\mathbb{B}(n)} \cdots \sum_{P_k\in\mathbb{B}(n)} \sum_{A\in\mathbb{B}(n)} E(\Delta_k(\varphi(A);\mathbf{P}))$$

We have to consider the k-th difference operator of φ. By linearity of the difference operator and the definitions of φ in (6.3.2) and $g_{R,k}$ in (6.2.1) we get

$$\begin{aligned} E(\Delta_k(\varphi(A);\mathbf{P})) &= E\left(\Delta_k(h(A);\mathbf{P}) + \Delta_k\left(\frac{R}{M}f(A);\mathbf{P}\right)\right) \\ &= E\left(k!\alpha_k P_1\cdots P_k\right) g_{R,k}(A;\mathbf{P}), \end{aligned}$$

where α_k is the leading coefficient of h. Thus

$$|S_n(\alpha)|^{2^k} \le (\#\mathbb{B}(n))^{2^k-k-1} \sum_{P_1\in\mathbb{B}(n)} \cdots \sum_{P_k\in\mathbb{B}(n)} E\left(k!\alpha_k P_1\cdots P_k\right) \sum_{A\in\mathbb{B}(n)} g_{R,k}(A;\mathbf{P}).$$

Taking the modulus and shifting to the innermost sum yields together with the definition of Φ in (6.2.2)

$$|S_n(h)|^{2^k} \leq (\#\mathbb{B}(n))^{2^k-k-1} \sum_{P_1\in\mathbb{B}(n)} \cdots \sum_{P_k\in\mathbb{B}(n)} |\Phi(\mathbf{P};n)|.$$

We apply Cauchy's inequality to get the modulus squared

$$|S_n(h)|^{2^{k+1}} \leq (\#\mathbb{B}(n))^{2^{k+1}-k-2} \sum_{P_1\in\mathbb{B}(n)} \cdots \sum_{P_k\in\mathbb{B}(n)} |\Phi(\mathbf{P};n)|^2 = (\#\mathbb{B}(n))^{2^{k+1}-k-2}\,\Psi_k(\mathbf{n};n).$$

Finally we apply Proposition 6.3 to estimate $\Psi_k(\mathbf{n};n)$. Thus

$$|S_n(h)|^{2^{k+1}} \ll (\#\mathbb{B}(n))^{2^{k+1}-k-2} \exp\left(-\frac{n}{a}\frac{1-|\Lambda(\mathbf{H})|^2}{q^{db}}\right)$$

and therefore

$$S_n(h) \ll (\#\mathbb{B}(n))^{1-\frac{k+2+\gamma}{2^{k+1}}},$$

where $\gamma > 0$ is defined by

$$(\#\mathbb{B}(n))^{-\gamma} = \exp\left(-\frac{n}{a}\frac{1-|\Lambda(\mathbf{H})|^2}{q^{db}}\right) \tag{6.3.3}$$

6.4 Waring's Problem

We have developed all our tools in order to treat Waring's Problem in $\mathbb{B}$ with digital restrictions.

Let $\mathcal{S} \subset \mathbb{B}$ and s be a positive integer. We call $\mathcal{S}$ a basis of $\mathbb{B}$ of order s if for every $N \in \mathbb{B}$ there is at least one representation of the form

$$N = P_1 + \cdots + P_s \quad \text{with } P_1,\ldots,P_s \in \mathcal{S}. \tag{6.4.1}$$

We call $\mathcal{S}$ an asymptotic basis if this is true for N of sufficiently large degree $d(N)$. For $\mathcal{S} := \{A^k : A \in \mathbb{B}\}$ the problem corresponds to the classical Waring's Problem and was considered by Car [10].

We want to extend this to representations of the shape

$$N = P_1^k + \cdots + P_s^k \quad \text{with } P_i \in \mathbb{B}(m) \text{ and } f(P_i) \equiv J \pmod{M} \tag{6.4.2}$$

where f is a Y-additive function and J and M are arbitrary polynomials in $\mathbb{B}$. This is a generalization of Theorem 5.5 in chapter 5.

Since the generalization of the classical Waring's Problem is due to Car [10] we want to follow this paper and therefore use her notation. We are looking for the smallest s, such that (6.4.2) has a solution for large N, *i.e.* $d(N)$ is large. Therefore we denote by $r(N,m,s,k)$ and $r(N,m,s,k,f,J,M)$ the number of solutions of the system in (6.4.1) and (6.4.2), respectively. If we additionally suppose that

$$k(m-1) < d(N) \leq km, \tag{6.4.3}$$

then we call $r(N,m,s,k) = R(N,s,k)$ and $r(N,m,s,k,f,J,M) = R(N,s,k,f,J,M)$ the number of strict representations of N.

We want to reduce our special case to the general one and therefore state the following proposition.

Proposition 6.6 ([10, Theorem]). *Let s be an integer such that $s \geq 1 + 2^k$. Then every $H \in \mathbb{B}$, such that $\deg(\mathrm{N}(H))$ is large enough, admits a strict representation as a sum of k-th powers. Moreover one has an asymptotic estimate for the number $R(N,s,k)$ of these representations.*

$$R(N,s,k) = q^{(s-1)(1-g-f)}\Theta_s(N)q^{(s-k)mf\mathfrak{S}_s(N)} + o(q^{(s-k)mf}),$$

where m is as in (6.4.3) *and* $0 < \Theta_s(N)\mathfrak{S}_s(N) \ll 1$.

As in [10] we denote by $\mathfrak{P}$ the valuation ideal of ν and by $\mathfrak{M}$ the valuation ideal of ω. Furthermore we write $\mathfrak{P}^{\otimes n} := \mathfrak{P} \times \cdots \times \mathfrak{P}$, with $\mathfrak{P}$ repeated n times. Let $\mathbf{b} := (b_1, \ldots, b_n)$ be an $\mathbb{A}$-basis of $\mathbb{B}$ and $\gamma = (\gamma_1, \ldots, \gamma_n)$ its dual basis. Then γ is a basis for $\mathcal{D}^{-1}$ (*cf.* [61, Chapter III,§3]). We define $h\gamma$ to be the isomorphism

$$h\gamma(t_1, \ldots, t_n) = (t_1\gamma_1 b_1, \ldots, t_n\gamma_n b_n).$$

We choose the Haar measures on $\mathbb{K}_\infty$ and $\mathbb{L}_\infty$ to be such that the values of the valuation ideals $\mathfrak{P}$ and $\mathfrak{M}$ equals 1, *i.e.* $\rho = \mathrm{d}x$ on $\mathbb{K}_\infty$ and μ on $\mathbb{L}_\infty$. We will always denote by $t = (t_1, \ldots, t_n)$ and element of $\mathbb{K}_\infty^n$ and by x one of $\mathbb{L}_\infty$. Finally on $\mathbb{K}_\infty^n$ we have the product measure $\rho^{\otimes n} = \mathrm{d}t_1 \times \cdots \times \mathrm{d}t_n = \mathrm{d}t$.

In order to count the solutions we will use the following Lemma.

Lemma 6.7 ([10, Proposition I.3.1]). *Let $H \in \mathbb{B}$. Then*

$$\int_{\mathfrak{P}^{\otimes n}} E(h\gamma(t) \cdot H)\mathrm{d}t = \begin{cases} 1 & \text{if } H = 0, \\ 0 & \text{else.} \end{cases}$$

For short we set for $z \in \mathbb{L}_\infty$, $m \geq 0$, $1 \leq i \leq s$, and $R \in \mathcal{D}^{-1}$

$$F(z,m) = \sum_{W \in \mathbb{B}(m)} E\left(zW^k\right),$$

$$S(z,m) = \sum_{\substack{W \in \mathbb{B}(m) \\ f(W) \equiv J \mod M}} E\left(zW^k\right),$$

$$H_R(z,m) = \sum_{W \in \mathbb{B}(m)} E\left(zW^k + \frac{R}{M}f(W)\right).$$

Thus we get the following integral representation for $R(N,m,s,k)$.

Lemma 6.8 ([10, Proposition II.1.2]).

$$R(N,s,k) = q^{1-g-f+\deg(D)} \int_{h\gamma(\mathfrak{P}^{\otimes n})} F(z,m)^s E(-zN)\mathrm{d}z.$$

We want to get from $S(z,m)$ to $H(z,m)$. Therefore we apply a trick which goes back to Gelfond [25] to connect the second and third sum.

$$S(z,m) = (\mathcal{N}(\mathbb{B}M))^{-1} \sum_{R \in \mathcal{R}(\mathbb{B}M)} \sum_{W \in \mathbb{B}(m)} E\left(zW^k + \frac{R}{M_i}(f(W) - J)\right)$$
$$= (\mathcal{N}(\mathbb{B}M))^{-1} \sum_{R \in \mathcal{R}(\mathbb{B}M)} E\left(-\frac{RJ}{M}\right) H_R(z,m).$$

In view of Lemma 6.8 we get that

$$R(N,s,k,f,J,M) = R'(N,s,k) = q^{1-g-f+\deg(D)} \int_{h\gamma(\mathfrak{P}^{\otimes n})} S(z,m)^s E(-zN)\mathrm{d}z$$

$$= q^{1-g-f+\deg(D)} \left(\mathcal{N}(\mathbb{B}M)\right)^{-s} \int_{h\gamma(\mathfrak{P}^{\otimes n})} \sum_{\mathbf{R}\in\mathcal{M}^s} \prod_{i=1}^{s} H_{R_i}(z,m) E\left(-\sum_{i=1}^{s} \frac{R_i J}{M} - zN\right) \mathrm{d}z.$$

We split the integral up into two parts according to whether $\mathbf{R} = 0$ or not. Thus

$$R'(N,s,k) = q^{1-g-f+\deg(D)} \left(\mathcal{N}(\mathbb{B}M)\right)^{-s} (I_1 + I_2),$$

where

$$I_1 = \int_{h\gamma(\mathfrak{P}^{\otimes n})} F(z,m)^s E(-zN)\mathrm{d}z = q^{g+f-1-\deg(D)} R(N,s,k),$$

$$I_2 = \int_{h\gamma(\mathfrak{P}^{\otimes n})} \sum_{\mathbf{0}\neq\mathbf{R}\in\mathcal{M}^s} \prod_{i=1}^{s} H_{R_i}(z,m) E\left(-\sum_{i=1}^{s} \frac{R_i J}{M} - zN\right) \mathrm{d}z.$$

In order to estimate the first integral we apply Proposition 6.6 and get

$$\left(\mathcal{N}(\mathbb{B}M)\right)^s I_1 = q^{(s-1)(1-g-f)} \Theta_s(N) q^{(s-k)mf} \mathfrak{S}_m(N) + o(q^{(s-k)mf}).$$

In order to proof our theorem we need to show that $I_2 = o(q^{(s-k)mf})$, *i.e.*, I_2 only contributes to the error term. Therefore we split the second integral I_2 up again according to the different values of $\mathbf{R}$. Thus

$$I_2 = \sum_{\mathbf{0}\neq\mathbf{R}\in\mathcal{M}^s} I_{\mathbf{R}},$$

where

$$I_{\mathbf{R}} = \int_{h\gamma(\mathfrak{P}^{\otimes n})} \prod_{i=1}^{s} H_{R_i}(z,m) E\left(-\sum_{i=1}^{s} \frac{R_i J}{M} - zN\right) \mathrm{d}z.$$

We split this integral up into two parts. Thus

$$|I_{\mathbf{R}}| \leq \sup_{R,z} |H_R(z,m)|^{s-2^k} \max_R \int_{h\gamma(\mathfrak{P}^{\otimes n})} H_R(z,m)^{2^k} \mathrm{d}z. \tag{6.4.4}$$

For the supremum we apply Theorem 6.1 to get

$$\sup_{R,z} |H_R(z,m)|^{s-2^k} \ll (\#\mathbb{B}(m))^{\left(s-2^k\right)\left(1-\frac{k+2+\gamma}{2^{k+1}}\right)}, \tag{6.4.5}$$

where γ is defined in (6.3.3) and $\mathbf{H} \in \mathcal{L}_b^k$ is such that

$$\left|\sum_{A\in\mathcal{L}_b} g_k(A;\mathbf{H})\right| < q^{db}.$$

We will apply Hua's Lemma to estimate the maximum. Therefore we need the following.

Lemma 6.9 ([10, Proposition II.5.2])**.** *Let c be any integer such that $1 \leq c \leq k$. Let $\varepsilon > 0$. Then*

$$\int_{h\gamma(\mathfrak{P}^{\otimes n})} F(z,m)^{2^c} E(-zN)\mathrm{d}z \ll (\#\mathbb{B}(m))^{2^c-c+\varepsilon}.$$

Thus we get by an application of Lemma 6.9

$$\max_R \int_{h\gamma(\mathfrak{P}^{\otimes n})} H_R(z,m)^{2^k} \mathrm{d}z \ll \max_R \int_{h\gamma(\mathfrak{P}^{\otimes n})} F(z,m)^{2^k} \mathrm{d}z \ll (\#\mathbb{B}(m))^{2^k-k+\varepsilon}. \tag{6.4.6}$$

Now plugging (6.4.5) and (6.4.6) into (6.4.4) yields

$$|I_{\mathbf{R}}| \ll (\#\mathbb{B}(m))^{\left(s-2^k\right)\left(1-\frac{k+2+\gamma}{2^{k+1}}\right)} (\#\mathbb{B}(m))^{2^k-k+\varepsilon} \ll (\#\mathbb{B}(m))^{s-k-\delta},$$

where ε has to be chosen such that

$$(s-2^k)\left(\frac{k+2+\gamma}{2^{k+1}}\right) - \varepsilon =: \delta > 0$$

which is possible since $s > 2^k$.

Thus a final application of (6.1.2) yields

$$I_2 = o\left((\#\mathbb{B}(m))^{(s-k)}\right) = o\left(q^{(s-k)mf}\right)$$

and the theorem is proven.

Remark 6.10. It is easy to generalize this result to the investigation of the following case

$$N = P_1^k + \cdots + P_s^k \quad (f_i(P_i) \equiv J_i \bmod M_i),$$

where every summand has its own Y-additive function f_i together with his own congruence relation $\equiv J_i \bmod M_i$. This can be done in quite the same way as in chapter 5 and is therefore left to the reader.

Bibliography

[1] T. M. Apostol, *Mathematical analysis: a modern approach to advanced calculus*, Addison-Wesley Publishing Company, Inc., Reading, Mass., 1957.

[2] G. I. Arkhipov, V. N. Chubarikov, and A. A. Karatsuba, *Trigonometric sums in number theory and analysis*, de Gruyter Expositions in Mathematics, vol. 39, Walter de Gruyter GmbH & Co. KG, Berlin, 2004, Translated from the 1987 Russian original.

[3] R. C. Baker, *Entire functions and uniform distribution modulo* 1, Proc. London Math. Soc. (3) **49** (1984), no. 1, 87–110.

[4] T. Beck, H. Brunotte, K. Scheicher, and J. M. Thuswaldner, *Number systems and tilings over Laurent series*, submitted, 2007.

[5] F. Blanchard and J.-M. Dumont, *Generic sequences, transducers and multiplication of normal numbers*, Israel J. Math. **80** (1992), no. 3, 257–287.

[6] E. Borel, *Les probabilités denombrables et leurs applications arithmétiques.*, Palermo Rend. **27** (1909), 247–271 (French).

[7] M. Car, *Le problème de Waring pour l'anneau des polynômes sur un corps fini*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A141–A144.

[8] ———, *Sommes de carrés de polynômes irréductibles dans* $\mathbf{F}_q[X]$, Acta Arith. **44** (1984), no. 4, 307–321.

[9] ———, *Sommes de puissances et d'irréductibles dans* $F_q[X]$, Acta Arith. **44** (1984), no. 1, 7–34.

[10] ———, *Waring's problem in function fields*, Proc. London Math. Soc. (3) **68** (1994), no. 1, 1–30.

[11] ———, *Répartition modulo* 1 *dans un corps de séries formelles sur un corps fini*, Acta Arith. **69** (1995), no. 3, 229–242.

[12] L. Carlitz, *Diophantine approximation in fields of characteristic* p, Trans. Amer. Math. Soc. **72** (1952), 187–208.

[13] P. T.-Y. Chern, *On meromorphic functions with finite logarithmic order*, Trans. Amer. Math. Soc. **358** (2006), no. 2, 473–489 (electronic).

[14] P. M. Cohn, *Algebraic numbers and algebraic functions*, Chapman and Hall Mathematics Series, Chapman & Hall, London, 1991.

[15] A. H. Copeland and P. Erdös, *Note on normal numbers*, Bull. Amer. Math. Soc. **52** (1946), 857–860.

[16] H. Davenport, *Multiplicative number theory*, second ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 1980, Revised by Hugh L. Montgomery.

[17] A. Dijksma, *Uniform distribution of polynomials over* GF$\{q, x\}$ *in* GF$[q, x]$. *I*, Nederl. Akad. Wetensch. Proc. Ser. A 72 = Indag. Math. **31** (1969), 376–383.

[18] ———, *Uniform distribution of polynomials over* GF$\{q,x\}$ *in* GF$[q,x]$. *II*, Nederl. Akad. Wetensch. Proc. Ser. A 73=Indag. Math. **32** (1970), 187–195.

[19] M. M. Dodson and S. Kristensen, *Hausdorff dimension and Diophantine approximation*, Fractal geometry and applications: a jubilee of Benoît Mandelbrot. Part 1, Proc. Sympos. Pure Math., vol. 72, Amer. Math. Soc., Providence, RI, 2004, pp. 305–347.

[20] M. Drmota and G. Gutenbrunner, *The joint distribution of Q-additive functions on polynomials over finite fields*, J. Théor. Nombres Bordeaux **17** (2005), no. 1, 125–150.

[21] M. Drmota and R. F. Tichy, *Sequences, discrepancies and applications*, Lecture Notes in Mathematics, vol. 1651, Springer-Verlag, Berlin, 1997.

[22] Jean-Marie Dumont and Alain Thomas, *Une modification multiplicative des nombres g normaux*, Ann. Fac. Sci. Toulouse Math. (5) **8** (1986/87), no. 3, 367–373.

[23] ———, *Modifications de nombres normaux par des transducteurs*, Acta Arith. **68** (1994), no. 2, 153–170.

[24] G. W. Effinger and D. R. Hayes, *Additive number theory of polynomials over a finite field*, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1991, , Oxford Science Publications.

[25] A. O. Gel′fond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*, Acta Arith. **13** (1967/1968), 259–265.

[26] B. Gittenberger and J. M. Thuswaldner, *Asymptotic normality of b-additive functions on polynomial sequences in the Gaussian number field*, J. Number Theory **84** (2000), no. 2, 317–341.

[27] P. J. Grabner, P. Kirschenhofer, and H. Prodinger, *The sum-of-digits function for complex bases*, J. London Math. Soc. (2) **57** (1998), no. 1, 20–40.

[28] S. W. Graham and G. Kolesnik, *van der Corput's method of exponential sums*, London Mathematical Society Lecture Note Series, vol. 126, Cambridge University Press, Cambridge, 1991.

[29] K. Gröchenig and A. Haas, *Self-similar lattice tilings*, J. Fourier Anal. Appl. **1** (1994), no. 2, 131–170.

[30] G. H. Hardy and J. E. Littlewood, *Some problems of diophantine approximation*, Acta Math. **37** (1914), no. 1, 193–239.

[31] ———, *A new solution of Waring's problem.*, Quart. J. **48** (1919), 272–293 (English).

[32] ———, *Some Problems of 'Partitio Numerorum'; I: A new solution of Waring's problem.*, Gtt. Nachr. (1920), 33–54 (English).

[33] D. R. Hayes, *The expression of a polynomial as a sum of three irreducibles*, Acta Arith. **11** (1966), 461–488.

[34] D. Hilbert, *Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem). Dem Andenken an Hermann Minkowski gewidmet.*, Math Ann. **67** (1909), 281–300 (German).

[35] J. H. Hodges, *Uniform distribution of sequences in* GF$[q, x]$, Acta Arith **12** (1966/1967), 55–75.

[36] L.-K. Hua, *On exponential sums over an algebraic number field*, Canadian J. Math. **3** (1951), 44–51.

[37] ______, *Additive Primzahltheorie*, B. G. Teubner Verlagsgesellschaft, Leipzig, 1959.

[38] K.-H. Indlekofer, I. Kátai, and P. Racskó, *Number systems and fractal geometry*, Probability theory and applications, Math. Appl., vol. 80, Kluwer Acad. Publ., Dordrecht, 1992, pp. 319–334.

[39] I. Kátai and B. Kovács, *Kanonische Zahlensysteme in der Theorie der quadratischen algebraischen Zahlen*, Acta Sci. Math. (Szeged) **42** (1980), no. 1-2, 99–107.

[40] ______, *Canonical number systems in imaginary quadratic fields*, Acta Math. Acad. Sci. Hungar. **37** (1981), no. 1-3, 159–164.

[41] I. Kátai and J. Szabó, *Canonical number systems for complex integers*, Acta Sci. Math. (Szeged) **37** (1975), no. 3-4, 255–260.

[42] D. E. Knuth, *The art of computer programming. Vol. 2*, second ed., Addison-Wesley Publishing Co., Reading, Mass., 1981, Seminumerical algorithms, Addison-Wesley Series in Computer Science and Information Processing.

[43] N. M. Korobov, *Exponential sums and their applications*, Mathematics and its Applications (Soviet Series), vol. 80, Kluwer Academic Publishers Group, Dordrecht, 1992, Translated from the 1989 Russian original by Yu. N. Shakhov.

[44] B. Kovács, *Canonical number systems in algebraic number fields*, Acta Math. Acad. Sci. Hungar. **37** (1981), no. 4, 405–407.

[45] B. Kovács and A. Pethő, *Number systems in integral domains, especially in orders of algebraic number fields*, Acta Sci. Math. (Szeged) **55** (1991), no. 3-4, 287–299.

[46] R. M. Kubota, *Waring's problem for* $\mathbf{F}_q[x]$, Dissertationes Math. (Rozprawy Mat.) **117** (1974), 60.

[47] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Interscience [John Wiley & Sons], New York, 1974, Pure and Applied Mathematics.

[48] M. G. Madritsch and J. M. Thuswaldner, *Waring's Problem in Function Fields with digital restrictions*, Preprint.

[49] ______, *Weyl Sums in* $\mathbb{F}_q[x]$ *with digital restrictions*, Preprint, submitted.

[50] M. G. Madritsch, J. M. Thuswaldner, and R. F. Tichy, *Normality of numbers generated by the values of entire functions*, J. Number Theory **128** (2008), no. 5, 1127–1145.

[51] Manfred G. Madritsch, *A note on normal numbers in matrix number systems*, Math. Pannon. **18** (2007), no. 2, 219–227.

[52] M.G. Madritsch, *Generating normal numbers over gaussian integers*, submitted.

[53] W. Müller, J. M. Thuswaldner, and R. F. Tichy, *Fractal properties of number systems*, Period. Math. Hungar. **42** (2001), no. 1-2, 51–68.

[54] Y. Nakai and I. Shiokawa, *Discrepancy estimates for a class of normal numbers*, Acta Arith. **62** (1992), no. 3, 271–284.

[55] ______, *Normality of numbers generated by the values of polynomials at primes*, Acta Arith. **81** (1997), no. 4, 345–356.

[56] M. B. Nathanson, *Additive number theory*, Graduate Texts in Mathematics, vol. 164, Springer-Verlag, New York, 1996, The classical bases.

[57] Q. I. Rahman, *On a class of integral functions of zero order*, J. London Math. Soc. **32** (1957), 109–110.

[58] K. Scheicher and J. M. Thuswaldner, *Canonical number systems, counting automata and fractals*, Math. Proc. Cambridge Philos. Soc. **133** (2002), no. 1, 163–182.

[59] ———, *Digit systems in polynomial rings over finite fields*, Finite Fields Appl. **9** (2003), no. 3, 322–333.

[60] J. Schiffer, *Discrepancy of normal numbers*, Acta Arith. **47** (1986), no. 2, 175–186.

[61] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1968, Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[62] C. L. Siegel, *Generalization of Waring's problem to algebraic number fields*, Amer. J. Math. **66** (1944), 122–136.

[63] Peter Szüsz and Bodo Volkmann, *A combinatorial method for constructing normal numbers*, Forum Math. **6** (1994), no. 4, 399–414.

[64] J. M. Thuswaldner, *Fractals and number systems in real quadratic number fields*, Acta Math. Hungar. **90** (2001), no. 3, 253–269.

[65] J. M. Thuswaldner and R. F. Tichy, *Waring's problem with digital restrictions*, Israel J. Math. **149** (2005), 317–344, Probability in mathematics.

[66] E. C. Titchmarsh, *The theory of functions*, Oxford University Press, London, 1975.

[67] E. C. Titchmarsh, *The theory of the Riemann zeta-function*, second ed., The Clarendon Press Oxford University Press, New York, 1986, Edited and with a preface by D. R. Heath-Brown.

[68] R. C. Vaughan, *The Hardy-Littlewood method*, second ed., Cambridge Tracts in Mathematics, vol. 125, Cambridge University Press, Cambridge, 1997.

[69] I. M. Vinogradov, *On Waring's problem*, Ann. of Math. (2) **36** (1935), no. 2, 395–405.

[70] ———, *Some theorems concerning the theory of primes.*, Rec. Math. Moscou, n. Ser. **2** (1937), 179–194 (English).

[71] ———, *On an estimate of trigonometric sums with prime numbers*, Izvestiya Akad. Nauk. SSSR. Ser. Mat. **12** (1948), 225–248.

[72] ———, *Selected works*, pp. 101–106, Springer-Verlag, 1985, On Waring's theorem.

[73] ———, *Selected works*, pp. 129–132, Springer-Verlag, 1985, Representation of an odd number as the sum of three primes.

[74] ———, *Selected works*, Springer-Verlag, Berlin, 1985, With a biography by K. K. Mardzhanishvili, Translated from the Russian by Naidu Psv [P. S. V. Naidu], Translation edited by Yu. A. Bakhturin.

[75] ———, *The method of trigonometrical sums in the theory of numbers*, Dover Publications Inc., Mineola, NY, 2004, Translated from the Russian, revised and annotated by K. F. Roth and Anne Davenport, Reprint of the 1954 translation.

[76] ———, *The method of trigonometrical sums in the theory of numbers*, Interscience Publishers, London and New York., no year given, Translated, revised and annotated by K. F. Roth and Anne Davenport.

[77] Bodo Volkmann, *On modifying constructed normal numbers*, Ann. Fac. Sci. Toulouse Math. (5) **1** (1979), no. 3, 269–285.

[78] ______, *À propos du théorème de Cassels-Schmidt concernant des nombres normaux*, Seminar on number theory, 1982–1983 (Talence, 1982/1983), Univ. Bordeaux I, Talence, 1983, pp. Exp. No. 30, 6.

[79] Bodo Volkmann and Peter Szüsz, *Sur des nombres normaux définis par un polynôme*, Séminaire de Théorie des Nombres, 1987–1988 (Talence, 1987–1988), Univ. Bordeaux I, Talence, 19??, pp. Exp. No. 42, 4.

[80] Y. Wang, *Diophantine equations and inequalities in algebraic number fields*, Springer-Verlag, Berlin, 1991.

[81] W. A. Webb, *Uniformly distributed functions in* $\mathrm{GF}[q, x]$ *and* $\mathrm{GF}\{q, x\}$, Ann. Mat. Pura Appl. (4) **95** (1973), 285–291.

[82] ______, *Waring's problem in* $\mathrm{GF}[q, x]$, Acta Arith. **22** (1973), 207–220.

[83] A. Weil, *Basic number theory*, Classics in Mathematics, Springer-Verlag, Berlin, 1995, Reprint of the second (1973) edition.

[84] H. Weyl, *Über die Gleichverteilung von Zahlen mod. Eins.*, Math. Ann. **77** (1916), 313–352 (German).