ASYMPTOTIC NORMALITY OF ADDITIVE FUNCTIONS ON POLYNOMIAL SEQUENCES IN CANONICAL NUMBER SYSTEMS

MANFRED G. MADRITSCH AND ATTILA PETHŐ

ABSTRACT. The objective of this paper is the study of functions which only act on the digits of an expansion. In particular, we are interested in the asymptotic distribution of the values of these functions. The presented result is an extension and generalization of a result of Bassily and Kátai to number systems defined in a quotient ring of the ring of polynomials over the integers.

1. INTRODUCTION

In this paper we investigate the asymptotic behaviour of q-additive functions. But before we start we need an idea of additive functions and the number systems they are living in. Note that a function f is said to be q-additive if it acts only on the q-adic digits, *i.e.*, $f(0) = 0$ and

$$f(n) = \sum_{h=0}^{\ell} f(a_h(n)q^h) \quad \text{for} \quad n = \sum_{h=0}^{\ell} a_h(n)q^h,$$

where $a_h(n) \in \mathcal{N} := \{0, \ldots, q-1\}$ are the *digits* of the q-adic expansion of n.

One of the first results dealing with the asymptotic behavior of such a q-additive function is the following, which is due to Bassily and Kátai [3].

Theorem. *Let f be a q-additive function such that $f(aq^h) = \mathcal{O}(1)$ as $h \to \infty$ and $a \in \mathcal{N}$. Furthermore let*

$$m_{h,q} := \frac{1}{q} \sum_{a \in \mathcal{N}} f(aq^h), \quad \sigma_{h,q}^2 := \frac{1}{q} \sum_{a \in \mathcal{N}} f^2(aq^h) - m_{h,q}^2,$$

and

$$M_q(x) := \sum_{h=0}^{N} m_{h,q}, \quad D_q^2(x) = \sum_{h=0}^{N} \sigma_{h,q}^2$$

with $N = [\log_q x]$. Assume that $D_q(x)/(\log x)^{1/3} \to \infty$ as $x \to \infty$ and let P be a polynomial with integer coefficients, degree d and positive leading term. Then, as $x \to \infty$,

$$\frac{1}{x} \# \left\{ n < x \left| \frac{f(P(n)) - M_q(x^d)}{D_q(x^d)} < y \right. \right\} \to \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y} \exp(-x^2) \mathrm{d}x.$$

A first step towards a generalization of this concept is based on number systems living in an order in an algebraic number field.

Definition 1.1. Let $\mathcal{R}$ be an integral domain, $b \in \mathcal{R}$, and $\mathcal{N} = \{n_1, \ldots, n_m\} \subset \mathbb{Z}$. Then we call the pair $(b, \mathcal{N})$ a *number system* in $\mathcal{R}$ if every $g \in \mathcal{R}$ admits a unique and finite representation of the form

$$g = \sum_{h=0}^{\ell} a_h(g) b^h \quad \text{with} \quad a_h(g) \in \mathcal{N}$$

and $a_h(g) \neq 0$ if $h \neq 0$. We call b the *base* and $\mathcal{N}$ the *set of digits*.

If $\mathcal{N} = \mathcal{N}_0 = \{0, 1, \ldots, m\}$ for $m \geq 1$ then we call the pair $(b, \mathcal{N})$ a *canonical number system*.

When extending the number system to the complex plane one has to face effects such as amenability, *i.e.*, there may exist two or more different expansions of one number. In fact, one can construct a graph (the connection graph) which characterizes all the amenable expansions. This has been done by Müller *et al.* [16] (with a direct approach) and by Scheicher and Thuswaldner [18] (consideration of the odometer).

A different view on digits in number systems is done by normal numbers. These are numbers in which expansion every possible block occurs asymptotically equally often. Constructions of such numbers have been considered by Dumont *et al.* [5] and the first author in [13, 14]

In this paper we mainly concentrate on additive functions. Thus we define additive functions in these number systems as follows.

Definition 1.2. Let $(b, \mathcal{N})$ be a number system in the integral domain $\mathcal{R}$. A function f is called *b-additive* if $f(0) = 0$ and

$$f(g) = \sum_{h \geq 0} f(a_h(g)b^h) \quad \text{for} \quad g = \sum_{h=0}^{\ell} a_h(g)b^h.$$

The simplest version of an additive function is the sum-of-digits function s_b defined by

$$s_b(g) := \sum_{h \geq 0} a_k(g).$$

The result by Bassily and Kátai was first generalized to number systems in the Gaussian integers by Gittenberger and Thuswaldner [7] who gained the following

Theorem. *Let $b \in \mathbb{Z}[i]$ and $(b, \mathcal{N})$ be a canonical number system in $\mathbb{Z}[i]$. Let f be a b-additive function such that $f(ab^h) = \mathcal{O}(1)$ as $h \to \infty$ and $a \in \mathcal{N}$. Furthermore let*

$$m_{h,b} := \frac{1}{\mathrm{N}(b)} \sum_{a \in \mathcal{N}} f(ab^h), \quad \sigma_{h,b}^2 := \frac{1}{\mathrm{N}(b)} \sum_{a \in \mathcal{N}} f^2(ab^h) - m_{h,b}^2,$$

and

$$M_b(x) := \sum_{h=0}^{L} m_{h,b}, \quad D_b^2(x) = \sum_{h=0}^{L} \sigma_{h,b}^2$$

with N the norm of an element over $\mathbb{Q}$ and $L = [\log_{\mathrm{N}(b)} x]$.

Assume that $D_b(x)/(\log x)^{1/3} \to \infty$ as $x \to \infty$ and let P be a polynomial of degree d with coefficients in $\mathbb{Z}[i]$. Then, as $N \to \infty$,

$$\frac{1}{\# \{z \in \mathbb{Z}[i] | \mathrm{N}(z) < N\}} \# \left\{ \mathrm{N}(z) < N \left| \frac{f(P(z)) - M_b(N^d)}{D_b(N^d)} < y \right. \right\} \to \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y} \exp(-x^2) \mathrm{d}x,$$

where N is the norm of an element over $\mathbb{Q}$ and z runs over the Gaussian integers.

This build the base for further considerations of *b*-additive functions in algebraic number fields in general. Therefore let $\mathcal{K} = \mathbb{Q}(\beta)$ be an algebraic number field and denote by $\mathcal{O}_\mathcal{K}$ its ring of integers (aka its maximal order). Furthermore let $\beta \in \mathcal{O}_\mathcal{K}$ then we set $\mathcal{R} = \mathbb{Z}[\beta]$ to be an order in $\mathcal{K}$. We now want to analyze additive functions for number systems in $\mathcal{R}$.

We need some more parameters in order to successfully generalize the theorem from above. Thus let $\mathcal{K}^{(\ell)}$ $(1 \leq \ell \leq r_1)$ be the real conjugates of $\mathcal{K}$, while $\mathcal{K}^{(m)}$ and $\mathcal{K}^{(m+r_2)}$ $(r_1 < m \leq r_1 + r_2)$ are the pairs of complex conjugates of $\mathcal{K}$, where $r_1 + 2r_2 = n$.

For $\gamma \in \mathcal{K}$ we denote by $\gamma^{(i)}$ $(1 \leq i \leq n)$ the conjugates of γ. In order to extend the term of conjugation to the completion $\overline{\mathcal{K}}$ of $\mathcal{K}$ we define for $\gamma_j \in \mathcal{K}$ and $x_j \in \mathbb{R}$ $(1 \leq j \leq n)$ $\lambda = \sum_{1 \leq j \leq n} x_j \gamma_j$ and $\lambda^{(i)} := \sum_{1 \leq j \leq n} x_j \gamma_j^{(i)}$.

Next we have to guarantee that we choose the increasing set for our asymptotic distribution. In the integer case we had the logarithm of the value, since the length of expansion growth with the logarithm. Since $\mathcal{R}$ is of dimension n we need a way to enlarge the area under consideration such that the expansion growth also in a smooth way. This is motivated by the following

Lemma 1.1 ([12, Theorem]). *Let $\ell(\gamma)$ be the length of the expansion of γ to the base b. Then*

$$\left| \ell(\gamma) - \max_{1 \leq i \leq n} \frac{\log \left| \gamma^{(i)} \right|}{\log \left| b^{(i)} \right|} \right| \leq C.$$

Therefore we define $\mathcal{R}(T_1, \ldots, T_r)$ to be the set

$$(1.1) \qquad \mathcal{R}(T_1, \ldots, T_r) := \left\{ \lambda \in \mathcal{R} : \left| \lambda^{(i)} \right| \leq T_i, 1 \leq i \leq r \right\}.$$

Now we use Lemma 1.1 to bound the area $\mathcal{R}(T_1, \ldots, T_n)$ such that we reach all elements of a certain length. Thus for a fixed T we set T_i for $1 \leq i \leq n$ such that

$$(1.2) \qquad \log T_i = \log T \frac{\log \left| b^{(i)} \right|^n}{\log |\mathrm{N}(b)|}.$$

Furthermore we will write for short $\mathcal{R}(\mathbf{T}) := \mathcal{R}(T_1, \ldots, T_r)$ with T_i as in (1.2).

Finally one can extend the definition of a number system also for negative powers of b. Then for $\gamma \in \overline{\mathcal{K}}$ such that

$$\gamma = \sum_{h=-\infty}^{\ell} a_h b^h \quad \text{with} \quad a_h \in \mathcal{N}$$

we call

$$\lfloor \gamma \rfloor := \sum_{h=0}^{h} a_h b^h \quad \text{and} \quad \{\gamma\} := \sum_{h \geq 1} a_h b^{-h}$$

the *integer part* and *fractional part* of γ, respectively.

With all these tools we now can state the generalization of the theorem of Bassily and Kátai to arbitrary number fields.

Theorem 1.2 ([15]). *Let $(b, \mathcal{N})$ be a number system in $\mathcal{R}$ and f be a b-additive function such that $f(ab^h) = \mathcal{O}(1)$ as $h \to \infty$ and $a \in \mathcal{N}$. Furthermore let*

$$m_{h,b} := \frac{1}{\mathrm{N}(b)} \sum_{a \in \mathcal{N}} f(ab^h), \quad \sigma_{h,b}^2 := \frac{1}{\mathrm{N}(b)} \sum_{a \in \mathcal{N}} f^2(ab^h) - m_{h,b}^2,$$

and

$$M_b(x) := \sum_{h=0}^{L} m_{h,q}, \quad D_b^2(x) = \sum_{h=0}^{L} \sigma_{h,q}^2$$

with $L = [\log_{\mathrm{N}(b)} x]$.

Assume that there exists an $\varepsilon > 0$ such that $D_b(x)/(\log x)^\varepsilon \to \infty$ as $x \to \infty$ and let $P \in \overline{\mathcal{K}}[X]$ be a polynomial of degree d. Then, as $T \to \infty$ let T_i be as in (1.2),

$$\frac{1}{\#\mathcal{R}(\mathbf{T})} \# \left\{ z \in \mathcal{R}(\mathbf{T}) \left| \frac{f(\lfloor P(z) \rfloor) - M_b(T^d)}{D_b(T^d)} < y \right. \right\} \to \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y} \exp(-x^2) \mathrm{d}x.$$

2. Definitions and result

The objective of this paper are generalizations of number systems to quotient rings of the ring of polynomials over the integers. Our aim is to extend Theorem 1.2 to such rings. To formulate our results we have to introduce the relevant notions. In particular we use the following definition in order to describe number systems in quotient rings of the ring of polynomials over the integers.

Definition 2.1. Let $p \in \mathbb{Z}[X]$ be monic of degree n and let $\mathcal{N}$ be a subset of $\mathbb{Z}$. The pair $(p, \mathcal{N})$ is called a number system if for every $g \in \mathbb{Z}[X] \setminus \{0\}$ there exist unique $\ell \in \mathbb{N}$ and $a_i \in \mathcal{N}, h = 0, \ldots, \ell; a_\ell \neq 0$ such that

$$(2.1) \qquad g \equiv \sum_{h=0}^{\ell} a_h(g) X^h \pmod{p}.$$

In this case a_i are called the digits and $\ell = \ell(a)$ the length of the representation.

This concept was introduced in [17] and was studied among others in [1, 2, 11, 12]. It was proved in [2], that $\mathcal{N}$ must be a complete residue system modulo $p(0)$ including 0 and the zeroes of p are lying outside or on the unit circle. However, following the argument of the proof of Theorem 6.1 of [17], which dealt with the case p square free, one can prove that non of the zeroes of p are lying on the unit circle.

If p is irreducible then we may replace X by one of the roots β of p. Then we are in the case of $\mathbb{Z}[X]/(p) \cong \mathbb{Z}[\beta]$ being an integral domain in an algebraic number field (*cf.* Section 1). Then we may also denote the number system by the pair $(\beta, \mathcal{N})$ instead of $(p, \mathcal{N})$. For example, let $q \geq 2$ be a positive integer, then $(p, \mathcal{N})$ with $p = X - q$ gives a number system in $\mathbb{Z}$, which corresponds to the number systems $(q, \mathcal{N})$. Furthermore for n a positive integer and $p = X^2 + 2n\,X + (n^2 + 1)$ we get number systems in $\mathbb{Z}[i]$.

Now we want to come back to these more general number systems and consider additive functions within them.

Definition 2.2. Let $(p, \mathcal{N})$ be a number system. A function f is called *additive* if $f(0) = 0$ and

$$f(g) \equiv \sum_{h=0}^{\ell} f(a_h(g)X^h) \pmod{p} \quad \text{for} \quad g \equiv \sum_{h=0}^{\ell} a_h(g)X^h \pmod{p}.$$

Since we have defined the analogues of number systems and additive functions to the definitions for number fields above, we now need to extend the length estimation of Lemma 1.1 in order to successfully state the result. But before we start we need a little linear algebra. We fix a number system $(p, \mathcal{N})$ and factor p by

$$p := \prod_{i=1}^{t} p_i^{m_i}$$

with $p_i \in \mathbb{Z}[X]$ irreducible and $\deg p_i = n_i$. Furthermore we denote by β_{ik} the roots of p_i for $i = 1, \ldots, t$ and $k = 1, \ldots, n_i$.

Then we define by

$$\mathcal{R} := \mathbb{Z}[X]/(p) = \bigoplus_{i=1}^{t} \mathcal{R}_i \quad \text{with} \quad \mathcal{R}_i = \mathbb{Z}[X]/\left(p_i^{m_i}\right)$$

for $i = 1, \ldots, t$ the $\mathbb{Z}$-module under consideration and in the same manner by

$$\mathcal{K} := \mathbb{Q}[X]/(p) = \bigoplus_{i=1}^{t} \mathcal{K}_i \quad \text{with} \quad \mathcal{K}_i = \mathbb{Q}[X]/\left(p_i^{m_i}\right)$$

for $i = 1, \ldots, t$ the corresponding vector space. Finally we denote by $\overline{\mathcal{K}}$ the completion of $\mathcal{K}$ according to the usual Euclidean distance.

Obviously $\mathcal{R}$ is a free $\mathbb{Z}$-module of rank n. Let $\lambda : \mathcal{R} \to \mathcal{R}$ be a linear mapping and $\{z_1, \ldots, z_n\}$ be any basis of $\mathcal{R}$. Then

$$\lambda(z_j) = \sum_{i=1}^{n} a_{ij} z_i \quad (j = 1, \ldots, n)$$

with $a_{ij} \in \mathbb{Z}$. The matrix $M(\lambda) = (a_{ij})$ is called the matrix of λ with respect to the basis $\{z_1, \ldots, z_n\}$. For an element $r \in \mathcal{R}$ we define by $\lambda_r : \mathcal{R} \to \mathcal{R}$ the mapping of multiplication by r; that is $\lambda_r(z) = rz$ for every $z \in \mathcal{R}$. Then we define the norm $\mathrm{N}(r)$ and the trace $\mathrm{Tr}(r)$ of an element $r \in \mathcal{R}$ as the determinant and the trace of $M(\lambda_r)$, respectively, *i.e.*,

$$\mathrm{N}(r) := \det(M(\lambda_r)), \quad \mathrm{Tr}(r) := \mathrm{Tr}(M(\lambda_r)).$$

Note that these are unique despite of the used basis $\{z_1, \ldots, z_n\}$. We can canonically extend these notions to $\mathcal{K}$ and $\overline{\mathcal{K}}$ by everywhere replacing $\mathbb{Z}$ by $\mathbb{Q}$ and $\mathbb{R}$, respectively.

In the following we will need parameters which help us bounding the length of the expansion of an element $g \in \mathcal{R}$. Therefore let $g \in \mathbb{Z}[X]$ be a polynomial, then we put

$$B_{ijk}(g) := \left.\frac{\mathrm{d}^{j-1}g}{\mathrm{d}X^{j-1}}\right|_{X=\beta_{ik}} \quad (i = 1, \ldots, t; j = 1, \ldots, m_i; k = 1, \ldots, n_i).$$

In connection with these values we define the "house" function H as

$$H(g) := \max_{i=1}^{t} \max_{j=1}^{m_i} \max_{k=1}^{n_i} |B_{ijk}(g)| .$$

We want to investigate the elements with bounded maximum length of expansion. To this end we need a proposition which estimates the length of expansion in connection with properties of the number itself. The proof of this proposition will be presented in the following section.

Proposition 2.1. *Assume that $(p, \mathcal{N})$ is a number system. Let $N = \max\{|a| : a \in \mathcal{N}\}$ and we set*

$$M(g) := \max \left\{ \frac{\log |B_{ijk}(g)|}{\log |\beta_{ik}|} : i = 1, \ldots, t; j = 1, \ldots, m_i; k = 1, \ldots, n_i \right\} .$$

If $g \in \mathbb{Z}[X]$ is of degree at most $n - 1$, then for any $\varepsilon > 0$ there exists $L = L(\varepsilon)$ such that if $\ell(g) > L$ then

$$(2.2) \qquad\qquad |\ell(g) - M(g)| \leq C.$$

This provides us with an estimation for the length of the expansion and motivates us to look at subsets of $\mathcal{R}$ where the absolute values B_{ijk} are bounded. For a vector $\mathbf{T} := (T_1, \ldots, T_n) = (T_{111}, \ldots, T_{11n_1}, T_{121}, \ldots, T_{1,m_i,n_1}, T_{211}, \ldots, T_{t,m_t,n_t})$ we denote by

$$(2.3) \qquad\qquad \mathcal{R}(\mathbf{T}) := \{g \in \mathcal{R} : |B_{ijk}(g)| \leq T_{ijk}\}$$

$$(2.4) \qquad\qquad \mathcal{R}_i(\mathbf{T}) := \{g \in \mathcal{R}_i : |B_{ijk}(g)| \leq T_{ijk}\} .$$

We want to let the length of expansion to smoothly increase. Therefore we fix a T and set T_{ijk} for $i = 1, \ldots, t$, $j = 1, \ldots, m_i$, $k = 1, \ldots, n_i$ such that

$$(2.5) \qquad\qquad \log T_{ijk} = \log T \frac{\log |\beta_{ik}|^n}{\log \prod_{i=1}^{t} \prod_{k=1}^{n_i} |\beta_{ik}|^{m_i}}.$$

Remark that T_{ijk} is independent from j, which will be important in Lemma 4.2. In view of Proposition 2.1 we get that the expansions of the elements in $\mathcal{R}(\mathbf{T})$ almost have the same maximum length. If not stated otherwise we denote by $\mathbf{T}$ the vector $(T_{111}, \ldots, T_{t,m_t,n_t})$ where the T_{ijk} are as in (2.5).

Since X is an invertible element in $\mathcal{K}$ we may extend the definition of a number system for negative powers of X. Then for $\gamma \in \overline{\mathcal{K}}$ such that

$$\gamma = \sum_{h=-\infty}^{\ell} a_h X^h \quad \text{with} \quad a_h \in \mathcal{N}$$

we call

$$\lfloor \gamma \rfloor := \sum_{h=0}^{\ell} a_h X^h \quad \text{and} \quad \{\gamma\} := \sum_{h=-\infty}^{-1} a_h X^h$$

the *integer part* and *fractional part* of γ, respectively.

Now we have collected all the tools to state our main result.

Theorem 2.2. *Let $(p, \mathcal{N})$ be a number system and f be an additive function such that $f(aX^h) = \mathcal{O}(1)$ as $h \to \infty$ and $a \in \mathcal{N}$. Furthermore let*

$$m_h := \frac{1}{|\mathcal{N}|} \sum_{a \in \mathcal{N}} f(aX^h), \quad \sigma_h^2 := \frac{1}{|\mathcal{N}|} \sum_{a \in \mathcal{N}} f^2(aX^h) - m_h^2,$$

and

$$M(x) := \sum_{h=0}^{L} m_h, \quad D^2(x) := \sum_{h=0}^{L} \sigma_h^2,$$

where $L = \lfloor \log_{p(0)} x \rfloor$. Assume that there exists an $\varepsilon > 0$ such that $D(x)/(\log x)^\varepsilon \to \infty$ as $x \to \infty$ and let $P \in \overline{\mathcal{K}}[Y]$ be a polynomial of degree d. Then, as $T \to \infty$ let T_{ijk} be as in (2.5),

$$\frac{1}{\#\mathcal{R}(T)} \# \left\{ z \in \mathcal{R}(T) : \frac{f(\lfloor P(z) \rfloor) - M(T^d)}{D(T^d)} < y \right\} \to \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y} \exp(-x^2) \mathrm{d}x.$$

Our theorem shows that the distribution properties of patterns in the sequence of digits depend neither on the polynomial p nor on the quotient ring $\mathcal{R}$. They are intimate properties of the "backward division algorithm" defined in [17].

We will show the main theorem in several steps.

(1) In the following section we will show properties of number systems which we need on the one hand to estimate the length of expansion and on the other hand to provide us with an Urysohn function, that helps us counting the occurrences of a fixed pattern of digits in the expansion.

(2) Equipped with these tools we will estimate the exponential sums occurring in the proof in Section 4. Therefore we need to split the module $\mathcal{R}$ up into its components and consider each of them separately. We also show that we may neglect the nilpotent elements.

(3) Now we take a closer look at the Urysohn function, which will count the occurences of our pattern in the expansion, and estimate the number of hits of the border of this function in Section 5. In particular, we count the number of hits of the area, where the function value lies between 0 and 1 as this area corresponds to the error term.

(4) In Section 6 we will show that any chosen patterns of digit and position occurs uniformly in the expansions. This will be our central tool in the proof of Theorem 2.2.

(5) Finally we draw all the thinks together. The main idea here is to use the growth rate of the deviation together with the Fréchet-Shohat Theorem to cut of the head and the tail of the expansion. Then an application of the central Proposition 5.1 and juxtaposition of the moments will prove the result.

3. Number system properties

In this section we want to show two properties we need in the sequel. The first deals with the above mentioned estimation of the length of an expansion (Proposition 2.1). We will need this result in order to justify our choice of $\mathbf{T}$ as in (2.5). Secondly we construct the Urysohn function for indicating the elements starting with a certain digit. The main idea is to embed the elements of $\mathcal{R}$ in $\mathbb{R}^n$ and to use the properties of matrix number systems in this field.

We start with the

Proof of Proposition 2.1. In the proof we combine ideas from [2] and [12].

We may assume $g \neq 0$. As $\{p, \mathcal{N}\}$ is a number system there are $\ell = \ell(A)$ and $a_h \in \mathcal{N}$ for $h = 0, \ldots, \ell;\, a_\ell \neq 0$ such that

$$g \equiv \sum_{h=0}^{\ell} a_h X^h \pmod{p},$$

i.e.,

$$g = \sum_{h=0}^{\ell} a_h X^h + r\,p$$

with a polynomial $r \in \mathbb{Z}[X]$. For $j \geq 1$ this implies

$$(3.1) \qquad \frac{\mathrm{d}^{j-1}g}{\mathrm{d}X^{j-1}} = \sum_{h=j-1}^{\ell} \frac{h!}{(h-j+1)!} a_h X^{h-j+1} + \sum_{s=0}^{j-1} \binom{j-1}{s} \frac{\mathrm{d}^s r}{\mathrm{d}X^s} \frac{\mathrm{d}^{j-1-s}p}{\mathrm{d}X^{j-1-s}}.$$

Consider a zero β_{ik} of p, which has multiplicity m_i. As we noticed in the Introduction, the argument of the proof of Theorem 6.1. of [17] allows to prove that $|\beta_{ik}| > 1$ for all $i = 1, \ldots, t;\, k = 1, \ldots, n_i$. Inserting β_{ik} into (3.1) we obtain

$$B_{ijk}(g) = \left.\frac{\mathrm{d}^{j-1}g}{\mathrm{d}X^{j-1}}\right|_{X=\beta_{ik}} = \sum_{h=j-1}^{\ell} \frac{h!}{(h-j+1)!} a_h \beta_{ik}^{h-j+1}$$

for $i = 1, \ldots, t$ and $j = 1, \ldots, m_i$. This implies by taking absolute value

$$
\begin{aligned}
|B_{ijk}(g)| &\leq N \sum_{h=j-1}^{\ell} \frac{h!}{(h-j+1)!} |\beta_{ik}|^{h-j+1} \\
&\leq N \frac{\ell!}{(\ell-j+1)!} |\beta_k^{\ell-j+1}| \sum_{h=j-1}^{\ell} \frac{h(h-1)\ldots(h-j+1)}{\ell(\ell-1)\ldots(\ell-j+1)} |\beta_{ik}|^{h-\ell} \\
&\leq N \frac{\ell^{j-1} |\beta_{ik}|^{\ell}}{|\beta_{ik}|-1},
\end{aligned}
$$

which verifies the lower bound for ℓ, because $|\beta_{ik}| > 1$.

Now we turn to prove the upper bound. Denote by $V = V_p$ the following mapping: for $g \in \mathbb{Z}[X]$ of degree at most $n-1$ choose an $a \in \mathcal{N}$ such that $g(0) \equiv a \pmod{p(0)}$. Such an a exists by Theorem 6.1 of [17]. Putting $q = \frac{g(0)-a}{p(0)}$, let $V(g) = \frac{g-q\cdot p-a}{X}$. Obviously $V(g) \in \mathbb{Z}[X]$ and has degree at most $n-1$, thus V can be iterated. Moreover we have

$$
(3.2) \qquad g \equiv \sum_{h=0}^{u} a_h X^h + X^{u+1} V^{u+1}(g) \pmod{p}
$$

with $a_h \in \mathcal{N}$ for $h = 0, \ldots, u$.

Choose u the largest integer satisfying $|B_{ijk}(g)| \geq \frac{u^j |\beta_{ik}|^{u-j+1}}{|\beta_{ik}|-1}$ for all $i = 1, \ldots, t$, $j = 1, \ldots, m_i$ and $k = 1, \ldots, n_i$. Then $u \leq (1 + \varepsilon/2) M(A)$. Proceeding like in the previous case we get

$$
\begin{aligned}
B_{ijk}(g) = \left. \frac{\mathrm{d}^{j-1} g}{\mathrm{d} X^{j-1}} \right|_{X=\beta_{ik}} &= \sum_{h=j}^{u} \frac{h!}{(h-j+1)!} a_h \beta_{ik}^{h-j} \\
&+ \sum_{s=0}^{j} \binom{j-1}{s} \frac{(u+1)!}{(u+1-s)!} \beta_{ik}^{u+1-s} \left. \frac{\mathrm{d}^{j-s-1} V^{u+1}(g)}{\mathrm{d} X^{j-s-1}} \right|_{X=\beta_{ik}}.
\end{aligned}
$$

By its definition $V^{u+1}(g)$ has integer coefficients. Dividing the last equation by $\frac{(u+1)!}{(u+1-j)!} \beta_{ik}^{u+1-j}$ and consider the obtained equations for $i = 1, \ldots, t$ and $k = 1, \ldots, n_i$ and for fixed i and k for $j = 1, \ldots, m_i$ successively, then using the choice of u and that $|\beta_{ik}| > 1$ we conclude that

$$
\left. \frac{\mathrm{d}^{j-s-1} V^{u+1}(g)}{\mathrm{d} X^{j-s-1}} \right|_{X=\beta_{ik}} < c,
$$

where c is a constant depending only on N as well as the size and the multiplicities of the zeroes of p. These can be considered as n inequalities for the n unknown coefficients of $V^{u+1}(g)$. Furthermore the determinant of the coefficient matrix is not zero (c.f. [2]). Thus the solutions are bounded. As they are integers there are only finitely many possibilities for $V^{u+1}(g)$. As $\{p, \mathcal{N}\}$ is a number system, $V^{u+1}(g)$ has a representation, which length is bounded by a constant, say c_1, which depends only on N as well as the size and the multiplicities of the zeroes of p. Thus $\ell(g) \leq u + c_1 \leq (1+\varepsilon) M(g)$ and the proposition is proved. □

Now we turn our attention back to the counting of the numbers and in particular to the construction of the Urysohn function. In order to properly count the elements we need the fundamental domain, which is defined as the set of all numbers whose integer part is zero. Since this is not so easy to define in this context we want to consider its embedding in $\mathbb{R}^n$. The main idea is to use the corresponding matrix of the polynomial p and to use properties of matrix number systems. This idea essentially goes back to Gröchenig and Haas [8]. The following definitions are standard in that area and we mainly follow Gittenberger and Thuswaldner [7] and Madritsch [15].

We note that if $(p, \mathcal{N})$ is a number system then X is a integral power base of $\overline{\mathcal{K}}$, i.e., $\{1, X, \ldots, X^{n-1}\}$ is an $\mathbb{R}$-basis for $\overline{\mathcal{K}}$. Thus we define the embedding ϕ by

$$
\phi : \begin{cases} \overline{\mathcal{K}} & \to & \mathbb{R}^n, \\ a_1 + a_2 X + \cdots + a_n X^{n-1} & \mapsto & (a_1, \ldots, a_n). \end{cases}
$$

Now let $p = b_{n-1}X^{n-1} + \cdots + b_1 X + b_0$. Then we define the corresponding matrix B by

(3.3)
$$B = \begin{pmatrix} 0 & 0 & \cdots & \cdots & \cdots & -b_0 \\ 1 & 0 & \cdots & \cdots & 0 & \vdots \\ 0 & 1 & \ddots & & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & 1 & 0 & \vdots \\ 0 & 0 & \cdots & 0 & 1 & -b_{n-1} \end{pmatrix}.$$

One easily checks that $\phi(X \cdot A) = B \cdot \phi(A)$. Since B is invertible we can extend the definition of ϕ by setting for an integer h

(3.4)
$$\phi(X^h \cdot A) := B^h \phi(A).$$

By this we define the (embedded) fundamental domain by

$$\mathcal{F} := \left\{ z \in \mathbb{R}^n \,\middle|\, z = \sum_{h \geq 1} B^{-h} a_h, a_h \in \phi(\mathcal{N}) \right\}.$$

Following Gröchenig and Haas [8] we get that

$$\lambda((\mathcal{F} + g_1) \cap (\mathcal{F} + g_2)) = 0$$

for every $g_1, g_2 \in \mathbb{Z}^n$ with $g_1 \neq g_2$, where λ denotes the n dimensional Lebesgue measure. Thus $(B, \phi(\mathcal{N}))$ is a matrix number system and a so called *just touching covering system*. Therefore we are allowed to apply the results of the paper by Müller et al. [16].

We now follow the lines of Madritsch [15] where the ideas of Gittenberger and Thuswaldner [7] were combined with the results of Kátai and Környei [10] and Müller et al. [16].

Our main interest is the fundamental domain consisting of all numbers whose first digit equals $a \in \mathcal{N}$, i.e.,

$$\mathcal{F}_a = B^{-1}(\mathcal{F} + \phi(a)).$$

Imitating the proof of Lemma 3.1 of [7] we get the following.

Lemma 3.1. *For all $a \in \mathcal{N}$ and all $v \in \mathbb{N}$ there exist a $1 \leq \mu < |\det B|$ and an axe-parallel tube $P_{v,a}$ with the following properties:*

- *$\partial \mathcal{F}_a \subset P_{v,a}$ for all $v \in \mathbb{N}$,*
- *the Lebesgue measure of $P_{v,a}$ is a $\mathcal{O}\left(\frac{\mu^v}{|\det B|^v}\right)$,*
- *$P_{v,a}$ consists of $\mathcal{O}(\mu^v)$ axe-parallel rectangles, each of which has Lebesgue measure $\mathcal{O}(|\det B|^v)$,*

where λ denotes the Lebesgue measure.

As in the proof of Lemma 3.1 of [7] we can construct for each pair (v, a) an axe-parallel polygon $\Pi_{v,a}$ and the corresponding tube

$$P_{v,a} := \left\{ z \in \mathbb{R}^n \,\middle|\, \|z - \Pi_{v,a}\|_\infty \leq 2c_p |\det B|^{-v} \right\},$$

where c_p is an arbitrary constant. Furthermore we denote by $I_{v,a}$ the set of all points inside $\Pi_{v,a}$. Now we define our Urysohn function u_a by

(3.5)
$$u_a(x_1, \ldots, x_n) = \frac{1}{\kappa^n} \int_{-\frac{\kappa}{2}}^{\frac{\kappa}{2}} \cdots \int_{-\frac{\kappa}{2}}^{\frac{\kappa}{2}} \psi_a(x_1 + y_1, \ldots, x_n + y_n) \, dy_1 \cdots dy_n,$$

where

(3.6)
$$\kappa := 2c_u |\det B|^{-v}$$

with c_u a constant and

$$\psi_a(x_1, \ldots, x_n) = \begin{cases} 1 & \text{if } (x_1, \ldots, x_n) \in I_{v,a} \\ \frac{1}{2} & \text{if } (x_1, \ldots, x_n) \in \Pi_{v,a} \\ 0 & \text{otherwise.} \end{cases}$$

Thus u_a is the desired Urysohn function which equals 1 for $z \in I_{v,a} \setminus P_{v,a}$, 0 for $z \in \mathbb{R}^n \setminus (I_{v,a} \cup P_{v,a})$, and linear interpolation in between.

We now do a Fourier transform of u_a and estimate the coefficients in the same way as in Lemma 3.2 of [7].

Lemma 3.2. *Let* $u_a(x_1, \ldots, x_n) = \sum_{(m_1, \ldots, m_n) \in \mathbb{Z}^n} c_{m_1, \ldots, m_n} e(m_1 x_1 + \cdots + m_n x_n)$ *be the Fourier series of* u_a. *Then the Fourier coefficients* $c_{m_1, \ldots, m_n}$ *can be estimated by*

$$c_{0, \ldots, 0} = \frac{1}{|\det B|}, \quad c_{m_1, \ldots, m_n} \ll \mu^v \prod_{i=1}^n \frac{1}{r(m_i)}$$

with

$$r(m_i) = \begin{cases} \kappa m_i & m_i \neq 0, \\ 1 & m_i = 0. \end{cases}$$

4. Estimation of the Weyl Sum

Before we continue with the estimation of the number of points inside the fundamental domain and those hitting the boarder, we want to estimate the exponential sums, which will occur in the following sections. In particular we want to prove the following.

Proposition 4.1. *Let* $T \geq 0$ *and* T_{ijk} *as in (2.5). Let* L *be the maximum length of the b-adic expansion of* $z \in \mathcal{R}(\mathbf{T})$ *and let* C_1 *and* C_2 *be sufficiently large constants. Furthermore let* $l_1, \ldots, l_h$ *be positions and* $\mathbf{h}_1, \ldots, \mathbf{h}_h$ *be corresponding n-dimensional vectors. If*

$$(4.1) \qquad\qquad C_1 \log L \leq l_1 < l_2 < \cdots < l_h \leq dL - C_2 \log L$$

and

$$(4.2) \qquad\qquad \|\mathbf{h}_r\|_\infty \leq (\log T)^{\sigma_1}$$

for $1 \leq r \leq h$, *then we have*

$$\sum_{z \in \mathcal{R}(\mathbf{T})} e\left(\sum_{r=1}^h \langle \mathbf{h}_r, B^{-l_r - 1} \phi(P(z)) \rangle\right) \ll T^n (\log T)^{-t \sigma_0}$$

where σ_0 *depends on* σ_1, C_1 *and* C_2.

Our main idea consists in several steps. First we will split the ring $\mathcal{R}$ up into the $\mathcal{R}_i$ and consider each of them separately. Then we distinguish two cases according to whether $m_i > 1$ or not. The latter reduces to an estimation of the sum in an algebraic number field. Whereas for the case of $m_i > 1$ we have to deal with nilpotent elements. Therefore we divide $\mathcal{R}_i$ into the radical and the nilpotent elements. Thus we define $\tilde{\mathcal{R}}_i$ as

$$(4.3) \qquad \tilde{\mathcal{R}}_i := \mathbb{Z}[X]/(p_i) \quad \text{and} \quad \tilde{\mathcal{R}}_i(\mathbf{T}) := \left\{ g \in \tilde{\mathcal{R}}_i : |B_{ijk}(g)| \leq T_{ijk} \right\}$$

and the set $\mathcal{N}_i$ to be the nilpotent elments, *i.e.*,

$$(4.4) \qquad \mathcal{N}_i := \{ g \in \mathcal{R}_i : g \equiv 0 \bmod p_i \} \quad \text{and} \quad \mathcal{N}_i(\mathbf{T}) := \{ g \in \mathcal{R}_i(\mathbf{T}) : g \equiv 0 \bmod p_i \}.$$

But before we start with the proof we need to show that the estimation is good compared with the trivial one. Thus we will show the following.

Lemma 4.2. *Let T_{ijk} for $i = 1, \ldots, t$, $j = 1, \ldots, m_i$, $k = 1, \ldots, n_i$ be positive reals. Then*

$$\#\mathcal{R}(\mathbf{T}) = \prod_{i=1}^{t} \#\mathcal{R}_i(\mathbf{T}),$$

$$\#\mathcal{R}_i(\mathbf{T}) = c_i \left(\prod_{k=1}^{n_i} T_{i1k} \right)^{m_i} + \mathcal{O}\left(T_0^{m_i n_i - 1} \right),$$

$$\#\mathcal{N}_i(\mathbf{T}) = c_i \left(\prod_{k=1}^{n_i} T_{i1k} \right)^{m_i - 1} + \mathcal{O}\left(T_0^{(m_i - 1)n_i - 1} \right),$$

where

$$T_0 = \max_{i=1}^{t} \max(1, (T_{i11} \cdots T_{i,m_i,n_i})^{\frac{1}{m_i n_i}})$$

and the constants c_i will be defined in Lemma 4.3.

Proof. The first assertion follows immediately from the definition of $\mathcal{R}(\mathbf{T})$. Since the $\mathcal{R}_i$ are independent we fix an i and focus on $\mathcal{R}_i(\mathbf{T})$. Obviously we have that

(4.5) $$\mathcal{R}_i = \mathbb{Z}[X]/(p_i^{m_i}) \cong (\mathbb{Z}[X]/(p_i))^{m_i}.$$

Thus we concentrate on $\mathbb{Z}[X]/(p_i\mathbb{Z}[X])$ which is an order in a number field $\mathcal{K}_i$ of degree n_i over $\mathbb{Q}$. For $\gamma \in \mathcal{K}_i$ let $\gamma^{(\ell)}$ $(1 \leq \ell \leq r_1)$ be the real conjugates and $\gamma^{(m)}$ and $\gamma^{(m+r_2)}$ $(r_1 + 1 \leq m \leq r_1 + r_2)$ be the pairs of complex conjugates of γ. Note that $r_1 + 2r_2 = n_i$. We will apply the following lemma.

Lemma 4.3 ([15, Lemma 3.3]). *Let T_k $(1 \leq k \leq r_1 + r_2)$ be positive integers and set $T_{r_1+r_2+k} = T_{r_1+k}$ for $1 \leq k \leq r_2$. Then*

$$\# \left\{ a \in \mathbb{Z}[X]/(p_i) : \left| a^{(k)} \right| \leq T_k \right\} = c_i T_1 \cdots T_{n_i} + \mathcal{O}\left(T_0^{n_i - 1} \right),$$

where $T_0 = \max\left(1, (T_1 \cdots T_{n_i})^{1/n_i}\right)$ and c_i is a constant depending on $\mathbb{Z}[X]/(p_i)$.

Furthermore since (4.5) holds, we get that there exists a $\mathbb{Z}$ linear mapping M_i such that

$$M_i \cdot (T_{i11}, \ldots, T_{i,m_i,n_i}) = (\tilde{T}_{i11}, \ldots, \tilde{T}_{i,m_i,n_i})$$

and

$$\#\mathcal{R}_i(\mathbf{T}) = \prod_{j=1}^{m_i} \# \left\{ a \in \mathbb{Z}[X]/(p_i) : \left| a^{(k)} \right| \leq \tilde{T}_{ijk} \quad 1 \leq k \leq n_i \right\}.$$

As the value of T_{ijk} is independent from j, an application of Lemma 4.3 yields

$$\#\mathcal{R}_i(\mathbf{T}) = \tilde{c}_i \left(\prod_{k=1}^{n_i} T_{i1k} \right)^{m_i} + \mathcal{O}\left(T_{i0}^{m_i n_i - 1} \right),$$

where $\tilde{c}_i$ depends on c_i and M_i and

$$T_{i0} = \max\left(1, (T_{i11} \cdots T_{i,m_i,n_i})^{\frac{1}{m_i n_i}} \right).$$

For the estimate involving $\mathcal{N}_i(\mathbf{T})$ we note that

$$\mathcal{N}_i = \{ g \in \mathcal{R}_i : g \equiv 0 \mod p_i \} \cong (\mathbb{Z}[X]/(p_i))^{m_i - 1}$$

and the result follows in the same way as for $\mathcal{R}_i(\mathbf{T})$. $\square$

With help of all these tools we can show Proposition 4.1.

Proof of Proposition 4.1. The first step consists in splitting the sum over $\mathcal{R}(\mathbf{T})$ up into those over $\mathcal{R}_i(\mathbf{T})$. Therefore let $\pi_i : \mathcal{R} \to \mathcal{R}_i$ be the canonical projections. Then $\pi := (\pi_1, \ldots, \pi_t)$ is an isomorphism by the Chinese Remainder Theorem. Furthermore let ϕ_i be the embedding defined by

$$\phi_i : \begin{cases} \overline{\mathcal{K}_i} & \to & \mathbb{R}^{n_i m_i}, \\ a_1 + a_2 X + \cdots + a_{m_i n_i} X^{n_i m_i - 1} & \mapsto & (a_1, \ldots, a_{m_i n_i}) \end{cases}$$

for $i = 1, \ldots, t$. Finally we define the matrix M to be such that

$$M \cdot \phi(z) := (\phi_1 \circ \pi_1(z), \ldots, \phi_t \circ \pi_t(z)).$$

Furthermore we note that for $P_i := \pi_i \circ P$ and $l \in \mathbb{Z}$ we have

$$M \cdot \phi(P(z)X^l) = (\phi_1(P_1(z_1)X^l), \ldots, \phi_t(P(z_t)X^l)).$$

Thus

$$\sum_{z \in \mathcal{R}(\mathbf{T})} e\left(\sum_{r=1}^{h} \langle \mathbf{h}_r, \phi(P(z)X^{-l_r-1}) \rangle \right) = \prod_{i=1}^{t} \sum_{z_i \in \mathcal{R}_i(\mathbf{T})} e\left(\sum_{r=1}^{h} \langle \mathbf{h}_{ri}, \phi_i(P_i(z_i)X^{-l_r-1}) \rangle \right)$$

where $(\mathbf{h}_{r1}, \ldots, \mathbf{h}_{rt}) := \mathbf{h}_r M^{-1}$.

Now we will consider each sum over $\mathcal{R}_i(\mathbf{T})$ separately. Therefore we fix until the end of the proof an $1 \le i \le t$ and distinguish two cases according to whether $m_i = 1$ or not.

- **Case 1, $m_i = 1$:** In this case we set $\beta = \beta_{i1}$ and observe that $K = \mathcal{K}_i = \mathbb{Q}(\beta_{i1})$ and $\mathcal{R}_i \cong \mathbb{Z}[\beta]$. Furthermore let $\mathcal{O}_K$ be the maximum order aka the ring of integers of K, then clearly $\mathbb{Z}[\beta_{i1}] \subset \mathcal{O}_K$. We denote by $\beta_{ik} = \beta^{(k)}$ the conjugates of β. Now we will proceed as in the proof of Proposition 6.1 of Madritsch [15].

  Therefore we need some parameters of the field K and for short we set $n = n_i$ during this case. Then we order the conjugates by denoting with $\beta^{(k)}$ for $1 \le k \le r_1$ the real conjugates, whereas $\beta^{(k)}$ and $\beta^{(k+r_2)}$ denote the pairs of complex conjugates, where $n = r_1 + 2r_2$. Let Tr be the trace of an element of K over $\mathbb{Q}$, then we define

  (4.6) $$\tau(z) := \left(\mathrm{Tr}(z), \mathrm{Tr}(\beta z), \ldots, \mathrm{Tr}(\beta^{n-1}z) \right) = \Xi \phi_i(z),$$

  where $\Xi = VV^T$ and V is the Vandermonde matrix

  $$V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta & \beta^{(2)} & \cdots & (\beta^{(n)})^{n-1} \\ \vdots & \vdots & & \vdots \\ \beta^{n-1} & (\beta^{(2)})^{n-1} & \cdots & (\beta^{(n)})^{n-1} \end{pmatrix}.$$

  We set $(\tilde{h}_{r1}, \ldots, \tilde{h}_{rn}) := \mathbf{h}_{ri}\Xi^{-1}$ and note that

  $$\langle \mathbf{h}_{ri}, \phi_i(P_i(z_i)X^{-l_r-1}) \rangle = \mathbf{h}_{ri}^T \Xi^{-1} \tau(P_i(z_i)\beta^{-l_r-1}) = \mathrm{Tr}\left(\sum_{k=1}^{n} \tilde{h}_{rk}\beta^{k-l_r-2}P_i(z_i) \right).$$

  Thus we may rewrite the sum under consideration as follows

  $$\sum_{z \in \mathcal{R}_i(\mathbf{T})} e\left(\sum_{r=1}^{h} \langle \mathbf{h}_{ri}, \phi_i(P_i(z_i)X^{-l_r-1}) \rangle \right) = \sum_{z \in \mathcal{R}_i(\mathbf{T})} e\left(\mathrm{Tr}\left(\sum_{r=1}^{h}\sum_{k=1}^{n} \tilde{h}_{rk}\beta^{k-l_r-2}P_i(z_i) \right) \right).$$

  Now we need an approximation lemma which essentially goes back to Siegel [19]. Therefore let δ be the different of K over $\mathbb{Q}$ and Δ be the absolute value of the discriminant of K. Then we have the following.

  Lemma 4.4. *Let $N_1, \ldots, N_{r_1+r_2}$ be real numbers and let $N = \sqrt[n]{N_1 \cdots N_{r_1}(N_{r_1+1} \cdots N_{r_1+r_2})^2}$ be their geometric mean. Suppose that $N > \Delta^{\frac{1}{n}}$, then, corresponding to any $\xi \in K$, there exist $q \in \mathcal{O}_K$ and $a \in \delta^{-1}$ such that*

  $$\left| q^{(k)}\xi^{(k)} - a^{(k)} \right| < N_k^{-1}, \quad 0 < \left| q^{(k)} \right| \le N_k, \quad 1 \le k \le r_1 + r_2,$$

  $$\max\left(N_k \left| q^{(k)}\xi^{(k)} - a^{(k)} \right|, \left| q^{(k)} \right| \right) \ge \Delta^{-\frac{1}{2}}, \quad 1 \le k \le r_1 + r_2,$$

  and

  $$\mathrm{N}((q, a\delta)) \le \Delta^{\frac{1}{2}}.$$

For $1 \le r \le h$ we set ξ_r to be the leading coefficient of $\sum_{k=1}^{n} \tilde{h}_{rk} P_i(z)$. Then we apply Lemma 4.4 with $N_k = T_{i,1,k}^{d} (\log T)^{-\sigma_2}$ for $1 \le k \le r_1 + r_2$ in order to get that there exist $a \in \delta^{-1}$ and $q \in \mathcal{O}_K$ such that

$$\left| \sum_{r=1}^{h} \frac{\xi_r^{(k)}}{(\beta^{(k)})^{l_r+1}} q^{(k)} - a^{(k)} \right| < \frac{(\log T)^{\sigma_2}}{T_{i,1,k}^{d}} \quad \text{and} \quad 0 < \left| q^{(k)} \right| < \frac{T_{i,1,k}^{d}}{(\log T)^{\sigma_2}} \quad \text{for} \quad 1 \le k \le n.$$

Lemma 4.5 ([15, Proposition 3.2]). *Suppose that*

$$(4.7) \qquad Q(X) = \alpha_d X^d + \cdots + \alpha_1 X$$

is a polynomial of degree d with coefficients in K. If for the leading coefficient α_d there exist $a \in \delta^{-1}$ and $q \in \mathcal{O}_K$ as in Lemma 4.4 with $N_k = T_{i1k}^{d} (\log T)^{-\sigma_2}$ and

$$(\log T)^{\sigma_2} \le \left| q^{(k)} \right| \le T_{i1k}^{d} (\log T)^{-\sigma_2} \quad 1 \le k \le r_1 + r_2,$$

then

$$\sum_{x \in \mathcal{R}_i(\mathbf{T})} e(\mathrm{Tr}(Q(x))) \ll T^{n_i} (\log T)^{-\sigma_0}$$

with $\sigma_2 \ge 2^{d-1} \left(\sigma_0 + r 2^{2d} \right)$.

Now we distinguish several cases according to the quality of approximation by Lemma 4.4, which is represented by the size of $H(q)$:

— **Case 1.1,** $\mathrm{H}(q) \ge (\log T)^{\sigma_2}$: We apply Lemma 4.5 and get

$$\sum_{z_i \in \mathcal{R}_i(\mathbf{T})} E \left(\sum_{r=1}^{h} \sum_{k=1}^{n} \frac{\tilde{h}_{rk} P_i(z_i))}{\beta^{l_r+1}} \right) \ll T^n (\log T)^{-\sigma_0}.$$

— **Case 1.2,** $2 \le \mathrm{H}(q) < (\log T)^{\sigma_2}$: In the last two cases we need Minkowski's lattice theory (*cf.* [9]). Let λ_1 be the first successive minimum of the $\mathbb{Z}$-lattice δ^{-1}. Then we get

$$\left| \sum_{r=1}^{h} \frac{\xi_r^{(k)}}{(\beta^{(k)})^{l_r+1}} \right| \ge \left| \frac{a^{(k)}}{q^{(k)}} \right| - \frac{1}{\left| q^{(k)} \right|^2} \ge \lambda_1 \left(\frac{1}{\left| q^{(k)} \right|} - \frac{1}{\left| q^{(k)} \right|^2} \right) \ge \lambda_1 \frac{1}{2 \left| q^{(k)} \right|} \gg (\log T)^{-\sigma_2},$$

which implies

$$(\log T)^{\sigma_2} \ll \left| \sum_{r=1}^{h} \frac{\xi_r^{(k)}}{(\beta^{(k)})^{l_r+1}} \right| \le \frac{\sum_{r=1}^{h} \left| \xi_r^{(k)} \right|}{\left| \beta^{(k)} \right|^{l_1+1}}.$$

Since $\left| \beta^{(k)} \right| > 1$ and (4.2) we have

$$\left| \beta^{(k)} \right|^{l_1+1} \ll \left| \xi^{(k)} \right| (\log T)^{\sigma_2} \ll n (\log T)^{\sigma_2+\sigma_1},$$

which yields

$$l_1 \ll \frac{(\sigma_2 + \sigma_1)}{\log \left| \beta^{(k)} \right|} \log \log T$$

contradicting the lower bound of l_1 for sufficiently large C_1 in (4.1).

— **Case 1.3,** $0 < \mathrm{H}(q) < 2$: In this case we will again use Minkowski's lattice theory (*cf.* [9]). Let λ_1 be the first successive minimum of the $\mathbb{Z}$-lattice δ^{-1}, then we have to consider two subcases

* **Case 1.3.1,** $\mathrm{H} \left(\sum_{r=1}^{h} \frac{\xi_r}{\beta^{l_r+1}} q \right) \ge \frac{\lambda_1}{2}$: Let $1 \le k \le n$ be such that

$$\frac{\lambda_1}{2} \le \left| \sum_{r=1}^{h} \frac{\xi_r^{(k)}}{(\beta^{(k)})^{l_r+1}} q^{(k)} \right| \le \frac{\sum_{r=1}^{h} \left| \xi_r^{(k)} \right|}{\left| \beta^{(k)} \right|^{l_1+1}} \left| q^{(k)} \right|,$$

then

$$l_1 + 1 \ll \log \log T$$

again contradicts the lower bound of l_1 for sufficiently large C_1 in (4.1).

* **Case 1.3.2,** $\mathrm{H}\left(\sum_{r=1}^{h} \frac{\xi_r}{\beta^{l_r+1}} q\right) < \frac{\lambda_1}{2}$: By Minkowski's theorem (*cf.* [9]) we get that $a = 0$. Thus for $1 \leq k \leq n$

$$\left| \sum_{r=1}^{h} \frac{\xi_r^{(k)}}{(\beta^{(k)})^{l_r+1}} q^{(k)} \right| = \left| \frac{1}{(\beta^{(k)})^{l_r+1}} \sum_{r=1}^{h} \xi_r^{(k)} (\beta^{(k)})^{l_h - l_r} q^{(k)} \right| \leq \frac{(\log T)^{\sigma_2}}{T_{i1k}^d}$$

which implies (taking the norm of the left side)

$$l_h + 1 \geq nd \log_{|\mathrm{N}(\beta)|} T - c(\log \log_{|\mathrm{N}(\beta)|} T)$$

contradicting the upper bound for sufficiently large C_2.

- **Case 2,** $m_i > 1$: Now we have to go one step further and to take a closer look at $\mathcal{R}_i$. In particular we divide every element $z_i \in \mathcal{R}_i$ into its radical and its nilpotent part. We fix an element $z \in \mathcal{R}$ and set $z_i := \pi_i(z)$.

On the one hand, since $\mathcal{R}_i = \tilde{\mathcal{R}}_i \oplus \mathcal{N}_i$ we have for $z_i \in \mathcal{R}_i$ the unique representation

(4.8) $$z_i = z_{i1} + z_{i2}$$

with $z_{i1} \in \tilde{\mathcal{R}}_i$ and $z_{i2} \in \mathcal{N}_i$. This motivates the definition of the linear map π_{ij} such that $\pi_{ij}(z) := z_{ij}$ for $i = 1, \dots, t$ and $j = 1, 2$.

On the other hand, since $\mathcal{R}_i \cong (\mathbb{Z}[X]/(p_i))^{m_i}$ we have for every $z_i \in \mathcal{R}_i$ the unique representation

$$z_i = \sum_{j=1}^{m_i} a_{ij} p_i^{j-1} = \sum_{j=1}^{m_i} \sum_{k=1}^{n_i} a_{ijk} X^{k-1} p_i^{j-1}$$

with $a_{ij} \in \mathbb{Z}[X]$ and $a_{ijk} \in \mathbb{Z}$, respectively. We clearly have

$$\pi_{i1}(z) = \sum_{k=1}^{n_i} a_{i1k} X^{k-1} \quad \text{and} \quad \pi_{i2}(z) = \sum_{j=2}^{m_i} \sum_{k=1}^{n_i} a_{ijk} X^{k-1} p_i^{j-1}.$$

Thus we define for $z_i \in \mathcal{R}_i$ the embeddings ψ_{i1} and ψ_{i2} by

$$\psi_{i1}(\pi_{i1}(z_i)) = (a_{i11}, \dots, a_{i1n_i}) \quad \text{and} \quad \psi_{i2}(\pi_{i2}(z_i)) = (a_{i21}, \dots, a_{i,m_i,n_i}).$$

Then there exists an invertible matrix $\tilde{M}_i$ such that

$$\tilde{M}_i(\phi_i \circ \pi_i(z)) = (\psi_{i1} \circ \pi_{i1}(z), \psi_{i2} \circ \pi_{i2}(z)).$$

Now we can divide the sum up as follows.

$$\sum_{z_i \in \mathcal{R}_i(\mathbf{T})} e\left(\sum_{r=1}^{h} \langle \mathbf{h}_{ri}, \phi_i(P_i(z_i) X^{-l_r-1}) \rangle \right)$$

$$= \sum_{z_{i1} \in \tilde{\mathcal{R}}_i(\mathbf{T})} \sum_{z_{i2} \in \mathcal{N}_i(\mathbf{T})} e\left(\sum_{r=1}^{h} \langle \mathbf{h}_{ri}, \phi_i(P_i(z_{i1} + z_{i2}) X^{-l_r-1}) \rangle \right)$$

$$= \sum_{z_{i1} \in \tilde{\mathcal{R}}_i(\mathbf{T})} e\left(\sum_{r=1}^{h} \langle \mathbf{h}_{ri1}, \psi_{i1}(P_{i1}(z_{i1}) X^{-l_r-1}) \rangle \right) \sum_{z_{i2} \in \mathcal{N}_i(\mathbf{T})} e\left(\sum_{r=1}^{h} \langle \mathbf{h}_{ri2}, \psi_{i2}(P_{i2}(z_{i2}) X^{-l_r-1}) \rangle \right),$$

where we have set $P_{ij} = \pi_{ij} \circ P$ for $j = 1, 2$.

Since for the first sum we have that $m_i = 1$ we may follow **Case 1** above and use Lemma 4.3 for trivially estimating the second one to prove the proposition for this case.

$\square$

5. Treatment of the border

In Section 3 above we have constructed the Urysohn function we need in order to properly count the number of elements within the fundamental domain. In this construction we also used an axe-parallel tube in order to cover the border of the fundamental domain. The number of hits of this tube gives rise to the error term which we will consider in this section.

We fix a positive integer v, which will be chosen later, and a real vector $\mathbf{T}$. Furthermore for $l \geq 0$ we define F_l to be the number of hits of the border of the Urysohn function which is

$$
(5.1) \qquad F_l := \# \left\{ z \in \mathcal{R}(\mathbf{T}) \,\middle|\, B^{-l-1} \phi\left(P(z)\right) \in \bigcup_{a \in \mathcal{N}} P_{v,a} \mod B^{-1}\mathbb{Z}^n \right\}.
$$

As indicated above we are interested in an estimation of F_l.

Proposition 5.1. *Let $\mu < |\det B|$ be as in Section 3 and C_1 and C_2 be sufficiently large positive reals. Suppose that l is a positive integer such that*

$$
(5.2) \qquad C_1 \log\log T \leq l \leq d \log_{|\det B|} T - C_2 \log\log T.
$$

Then for any positive σ_3 we have

$$
F_l \ll \mu^v T^n \left(|\det B|^{-v} + (\log T)^{-t\sigma_3} \right).
$$

In order to estimate F_l we need the Erdős-Turán-Koksma Inequality.

Lemma 5.2 ([4, Theorem 1.21]). *Let $x_1, \ldots, x_S$ be points in the n-dimensional real vector space $\mathbb{R}^n$ and H an arbitrary positive integer. Then the discrepancy $D_S(x_1, \ldots, x_S)$ fulfills the inequality*

$$
D_S(x_1, \ldots, x_S) \ll \frac{2}{H+1} + \sum_{0 < \|\mathbf{h}\|_\infty \leq H} \frac{1}{r(\mathbf{h})} \left| \frac{1}{S} \sum_{s=1}^{S} e(\langle \mathbf{h}, x_s \rangle) \right|,
$$

where $\mathbf{h} \in \mathbb{Z}^n$ and $r(\mathbf{h}) = \prod_{i=1}^{n} \max(1, |h_i|)$.

Proof of Proposition 5.1. We want to proceed in three steps. First we subdivide the tube $P_{v,a}$ into rectangles in order to apply the Erdős-Turán-Koksma Inequality in the second step. Finally we put them together to gain the desired result.

Recall that the tube $P_{v,a}$ defined in Lemma 3.1 consists of a family of rectangles. Let R_a be one of them, then we want to estimate

$$
F_l(R_a) := \# \left\{ z \in \mathcal{R}(\mathbf{T}) \,\middle|\, B^{-l-1} \phi\left(P(z)\right) \in \bigcup_{a \in \mathcal{N}} R_a \mod B^{-1}\mathbb{Z}^n \right\}.
$$

Using the definition of the discrepancy we get that

$$
(5.3) \qquad F_l(R_a) \ll T^n \left(\lambda(R_a) + D_S\left(\left\{ B^{-l-1}\phi\left(P(z)\right) \right\}_{z \in \mathcal{R}(\mathbf{T})} \right) \right),
$$

where λ is the n-dimensional Lebesgue measure and S is the number of elements in $\mathcal{R}(\mathbf{T})$. By Lemma 4.2 we have that

$$
(5.4) \qquad S = \prod_{i=1}^{t} c_i \left(\prod_{k=1}^{n_i} T_{i1k} \right)^{m_i} + \mathcal{O}\left(T_0^{n-1} \right).
$$

Now we apply Lemma 5.2 to get
$$
(5.5)
$$

$$
D_S\left(\left\{ B^{-l-1}\phi\left(P(z)\right) \right\}_{z \in \mathcal{R}(\mathbf{T})} \right) \ll \frac{2}{H+1} + \sum_{0 < \|\mathbf{h}\|_\infty \leq H} \frac{1}{r(\mathbf{h})} \left| \frac{1}{S} \sum_{z \in \mathcal{R}(\mathbf{T})} e\left(\langle \mathbf{h}, B^{-l-1}\phi\left(P(z)\right) \rangle \right) \right|.
$$

The next step consists in an application of Proposition 4.1 which yields

$$
(5.6) \qquad \left| \sum_{z \in \mathcal{R}(\mathbf{T})} e\left(\langle \mathbf{h}, B^{-l-1}\phi\left(P(z)\right) \rangle \right) \right| \ll T^n (\log T)^{-t\sigma_0}
$$

Putting (5.4), (5.5), and (5.6) togetter in (5.3) gives

$$F_l(R_a) \ll T^n \lambda(R_a) + \frac{T^n}{(\log T)^{\sigma_1}} + T^n (\log T)^{-t\sigma_0} \sum_{0 < \|\mathbf{h}\|_\infty \le H} \frac{1}{r(\mathbf{h})}$$

$$\ll T^n \lambda(R_a) + \frac{T^n}{(\log T)^{\sigma_1}} + T^n (\log T)^{-t\sigma_0} (\log \log T)^n.$$

Setting $\sigma_1 := t\sigma_0/2$ and summing over all rectangles R_a yields

$$F_l \ll \mu^v T^n \left(|\mathrm{N}(b)|^{-v} + (\log T)^{-t\sigma_0/2} \right).$$

Finally we set $\sigma_3 = t\sigma_0/2$ which proves the proposition. $\qquad\square$

6. The main proposition

The main idea is to understand the additive function as putting weights on the digits. Thus if we can show that the digits are uniformly distributed the same is true for the values of the additive functions. Therefore we look at patterns in the expansion of $P(z)$. In particular, we count the number of occurrences of certain digits at certain positions in the expansions.

Proposition 6.1. *Let f be an additive function. Let $T \ge 0$ and T_{ijk} as in (2.5). Let L be the maximum length of the b-adic expansion of $z \in \mathcal{R}(\mathbf{T})$ and let C_1 and C_2 be sufficiently large. Then for*

$$(6.1) \qquad C_1 \log L \le l_1 < l_2 < \cdots < l_h \le dL - C_2 \log L$$

we have,

$$\Theta := \# \left\{ z \in \mathcal{R}(\mathbf{T}) | a_{l_r}(f(z)) = b_r, r = 1, \ldots, h \right\}$$
$$= \frac{c_1 \cdots c_t}{|\det B|^h} T^n + \mathcal{O}\left(T^n (\log T)^{-t\sigma_0} \right).$$

uniformly for $T \to \infty$, where $(l_r, b_r) \in \mathbb{N} \times \mathcal{N}$ are given pairs of position and digit and σ_0 is an arbitrary positive constant.

Proof. We recall our Urysohn function u_a (defined in (3.5)) and set for $\nu \in \mathbb{R}^n$

$$t(\nu) = u_{b_1}(B^{-l_1-1}\nu) \cdots u_{b_h}(B^{-l_h-1}\nu),$$

where B is the matrix defined in (3.3).

Now we want to apply the Fourier transformation, which we developed in Lemma 3.2. Therefore we set

$$\mathcal{M} := \left\{ M = (h_1, \ldots, h_h) | h_r \in \mathbb{Z}^n, \text{ for } r = 1, \ldots, h \right\}.$$

An application of Lemma 3.2 yields

$$(6.2) \qquad t(\nu) = \sum_{M \in \mathcal{M}} T_M e\left(\sum_{r=1}^h \mathbf{h}_r B^{-l_r-1} \nu \right),$$

where $T_M = \prod_{r=1}^h c_{m_{r1}, \ldots, m_{rn}}$. Combining this with the definition of F_l in (5.1) we get

$$(6.3) \qquad \left| \Theta - \sum_{z \in \mathcal{R}(\mathbf{T})} t(\phi(P(z))) \right| \le F_{l_1} + \cdots + F_{l_h}.$$

Plugging (6.2) into (6.3) together with an application of Lemma 3.2 for the coefficients yields

$$\Theta = \frac{c_1 \cdots c_t}{|\det(B)|^h} T^n + \sum_{0 \ne M \in \mathcal{M}} T_M e\left(\sum_{r=1}^h \langle \mathbf{h}_r, B^{-l_r-1} \phi(P(z)) \rangle \right) + \mathcal{O}\left(\sum_{r=1}^h F_{l_r} \right).$$

Now an application of Proposition 4.1 to treat the exponential sums, of Proposition 5.1 for the border F_l with $v \ll \log \log T$ and the observation that

$$\sum_{M \in \mathcal{M}} |T_M| \ll \kappa^{-2h} \ll |\det B|^{2hv} \ll (\log T)^{t\sigma_0/2},$$

where we used the definition of κ in (3.6), proves the proposition. $\qquad \square$

7. Proof of Theorem 2.2

For this proof we mainly follow the proof of the Theorem of Bassily and Kátai [3]. In the same manner we cut of the head and tail of the expansion and show the theorem for a truncated version of the additive function. In particular we set $C := \max(C_1, C_2)$, $A := [C \log L]$ and $B := L - A$, where L, C_1 and C_2 are defined in the statement of Proposition 6.1. Furthermore we define the truncated function f' to be

$$f'(P(z)) = \sum_{j=A}^{B} f(a_j(P(z))b^j).$$

By the definition of A and $f(ab^j) \ll 1$ with $a \in \mathcal{N}$ we get that $f'(P(z)) = f(P(z)) + \mathcal{O}(\log L)$. In the same manner we define the truncated mean and standard deviation

$$M'(T) := \sum_{j=A}^{B} m_j \quad \text{and} \quad D'^2(T) := \sum_{j=A}^{B} \sigma_j^2.$$

At this point we need that the deviation D tends sufficiently fast do infinity. In particular, we could refine the statement, if we shrink the part, which is cut of. Since $M(T) - M'(T) = \mathcal{O}(\log L)$ and $D^2(T) - D'^2(T) = \mathcal{O}(\log L)$ we get that it suffices to show that

$$\frac{1}{\#\mathcal{R}(\mathbf{T})} \# \left\{ z \in \mathcal{R}(\mathbf{T}) \,\middle|\, \frac{f'(P(z)) - M'(T^d)}{D'(T^d)} < y \right\} \longrightarrow \Phi(y).$$

By the Fréchet-Shohat Theorem (*cf.* [6, Lemma 1.43]) this holds true if and only if the moments

$$\xi_k(T) := \frac{1}{\#\mathcal{R}(\mathbf{T})} \sum_{z \in \mathcal{R}(\mathbf{T})} \left(\frac{f'(P(z)) - M'(T^d)}{D'(T^d)} \right)^k$$

converge to the moments of the normal law for $T \to \infty$. We will show the last statement by comparing the moments ξ_k with

$$\eta_k(T) := \frac{1}{\#\mathcal{R}(\mathbf{T}^d)} \sum_{z \in N(T^d)} \left(\frac{f'(z) - M'(T^d)}{D'(T^d)} \right)^k,$$

where $\mathbf{T}^d = (T_1^d, \ldots, T_n^d) = (T_{111}^d, \ldots, T_{t,n_t,m_t}^d)$.

An application of Proposition 6.1 gives that

$$\xi_k(T) - \eta_k(T) \to 0 \quad \text{for} \quad T \to \infty.$$

Furthermore we get by Proposition 2.1 that these sums consist of independently identically distributed random variables (with possible $2C$ exceptions). By the central limit theorem we get that their distribution converges to the normal law. Thus the $\eta_k(T)$ converge to the moments of the normal law. This yields

$$\lim_{T \to \infty} \xi_k(T) = \lim_{T \to \infty} \eta_k(T) = \int x^k \mathrm{d}\Phi.$$

We apply the Fréchet-Shohat Theorem again to prove the theorem.

Acknowledgment

References

[1] S. Akiyama, T. Borbély, H. Brunotte, A. Pethő, and J. M. Thuswaldner, *Generalized radix representations and dynamical systems. I*, Acta Math. Hungar. **108** (2005), no. 3, 207–238.

[2] S. Akiyama and H. Rao, *New criteria for canonical number systems*, Acta Arith. **111** (2004), no. 1, 5–25.

[3] N. L. Bassily and I. Kátai, *Distribution of the values of q-additive functions on polynomial sequences*, Acta Math. Hungar. **68** (1995), no. 4, 353–361.

[4] M. Drmota and R. F. Tichy, *Sequences, discrepancies and applications*, Lecture Notes in Mathematics, vol. 1651, Springer-Verlag, Berlin, 1997.

[5] J. M. Dumont, P. J. Grabner, and A. Thomas, *Distribution of the digits in the expansions of rational integers in algebraic bases*, Acta Sci. Math. (Szeged) **65** (1999), no. 3-4, 469–492.

[6] P. D. T. A. Elliott, *Probabilistic number theory. I*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science], vol. 239, Springer-Verlag, New York, 1979, Mean-value theorems.

[7] 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.

[8] K. Gröchenig and A. Haas, *Self-similar lattice tilings*, J. Fourier Anal. Appl. **1** (1994), no. 2, 131–170.

[9] L.-K. Hua, *Introduction to number theory*, Springer-Verlag, Berlin, 1982, Translated from the Chinese by Peter Shiu.

[10] I. Kátai and I. Környei, *On number systems in algebraic number fields*, Publ. Math. Debrecen **41** (1992), no. 3-4, 289–294.

[11] 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.

[12] _____, *On a representation of algebraic integers*, Studia Sci. Math. Hungar. **27** (1992), no. 1-2, 169–172.

[13] M. G. Madritsch, *A note on normal numbers in matrix number systems*, Math. Pannon. **18** (2007), no. 2, 219–227.

[14] _____, *Generating normal numbers over Gaussian integers*, Acta Arith. **135** (2008), no. 1, 63–90.

[15] _____, *Asymptotic normality of b-additive functions on polynomial sequences in number systems*, Ramanujan J. **21** (2010), no. 2, 181–210.

[16] W. Müller, J. M. Thuswaldner, and R. F. Tichy, *Fractal properties of number systems*, Period. Math. Hungar. **42** (2001), no. 1-2, 51–68.

[17] A. Pethő, *On a polynomial transformation and its application to the construction of a public key cryptosystem*, Computational number theory (Debrecen, 1989), de Gruyter, Berlin, 1991, pp. 31–43.

[18] K. Scheicher and J. M. Thuswaldner, *Canonical number systems, counting automata and fractals*, Math. Proc. Cambridge Philos. Soc. **133** (2002), no. 1, 163–182.

[19] C. L. Siegel, *Generalization of Waring's problem to algebraic number fields*, Amer. J. Math. **66** (1944), 122–136.

(M. G. Madritsch) Department of Analysis and Computational Number Theory
Graz University of Technology
A-8010 Graz, Austria
E-mail address: madritsch@math.tugraz.at

(A. Pethő) Department of Computer Science, University of Debrecen,
Number Theory Research Group,
Hungarian Academy of Sciences and University of Debrecen
P.O. Box 12, H-4010 Debrecen, Hungary
E-mail address: petho.attila@inf.unideb.hu