WEYL SUMS IN $\mathbb{F}_q[x]$ WITH DIGITAL RESTRICTIONS

MANFRED G. MADRITSCH AND JÖRG M. THUSWALDNER

Abstract. Let $\mathbb{F}_q$ be a finite field and consider the polynomial ring $\mathbb{F}_q[X]$. Let $Q \in \mathbb{F}_q[X]$. A function $f : \mathbb{F}_q[X] \to G$, where G is a group, is called *strongly Q-additive*, if $f(AQ + B) = f(A) + f(B)$ holds for all polynomials $A, B \in \mathbb{F}_q[X]$ with $\deg B < \deg Q$. We estimate Weyl Sums in $\mathbb{F}_q[X]$ restricted by Q-additive functions. In particular, for a certain character E we study sums of the form

$$\sum_P E(h(P)),$$

where $h \in \mathbb{F}_q((X^{-1}))[Y]$ is a polynomial with coefficients contained in the field of formal Laurent series over $\mathbb{F}_q$ and the range of P is restricted by conditions on $f_i(P)$, where f_i $(1 \le i \le r)$ are Q_i-additive functions. Adopting an idea of Gel′fond such sums can be rewritten as sums of the form

$$\sum_{\deg P<n} E\left(h(P) + \sum_{i=1}^{r} \frac{R_i}{M_i} f_i(A)\right),$$

with $R_i, M_i \in \mathbb{F}_q[X]$. Sums of this shape are treated by applying the k-th iterate of the Weyl-van der Corput inequality and studying higher correlations of the functions f_i. With these Weyl Sum estimates we show uniform distribution results.

1. Introduction

The objective of the present paper 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 $\mathcal{R} := \mathbb{F}_q[X]$. In order to describe this more precisely, let

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

be the set of all polynomials in $\mathcal{R}$ whose degree is less than n and fix a polynomial $Q \in \mathcal{R}$ of positive degree d. It is easy to see that each $A \in \mathcal{R}$ admits a unique *Q-ary digital expansion*

$$A = \sum_{i\ge 0} D_i Q^i \qquad (D_i \in \mathcal{P}_d). \tag{1.1}$$

We call a function $f : \mathcal{R} \to G$, where G is a group, strongly Q-additive if $f(AQ+B) = f(A)+f(B)$. Thus, if we represent an element $A \in \mathcal{R}$ by its Q-ary digital expansion (1.1), we may write

$$f(A) = \sum_{i\ge 0} f(D_i).$$

One simple example is the *sum of digits function*, which is defined by

$$s_Q(A) := \sum_{i\ge 0} D_i.$$

Drmota and Gutenbrunner [6] considered exponential sums of the shape

$$\sum_{A\in\mathcal{P}_n} E\left(\sum_{i=1}^{r} \frac{R_i}{M_i} f_i(A)\right) \tag{1.2}$$

Date: May 20, 2008.

2000 *Mathematics Subject Classification.* 11T23, 11A63.

Key words and phrases. Finite fields, digit expansions, Weyl sums, uniform distribution, Waring's Problem.

Supported by the Austrian Research Foundation (FWF), Projects S9603, S9610 and S9611, that are part of the Austrian Research Network "Analytic Combinatorics and Probabilistic Number Theory".

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 (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 (1.2) may contain an additional polynomial summand. This result also forms a generalization of a result of Kubota [11] which is the basis of a treatment of Waring's Problem in function fields. We will dwell on this result again in Section 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. In particular, the present paper is organized as follows.

- In Section 2 we define the basic notions which are standard in this area (*cf.* for instance [1, 3, 4, 5, 9, 11]) and give some preliminary results. Moreover we state the main results of the paper, *i.e.*, an estimates for Weyl sums in $\mathcal{R}$ with Q_i-additive functions and an equidistribution result in $\mathbb{F}_q$ involving rstrictions by Q_i-additive functions.
- Section 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 [6].
- Section 4 is devoted to the proof of the Weyl sum estimates. To this matter the correlation result of the previous section is used.
- Section 5 contains the proof of the uniform distribution result.

2. Preliminaries and statement of results

We want to state our results on Weyl Sums over the ring $\mathcal{R} := \mathbb{F}_q[X]$ 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 $\mathbb{F}_q$. All these objects are standard in this field (see for instance [1, 11]) and we recall their definition briefly.

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.

With $\mathcal{R}$ and $\mathcal{K}$ we have the analogues 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 $A, B \in \mathcal{R}$, then

$$\nu(A/B) := \deg A - \deg B \tag{2.1}$$

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*.

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

$$E(\alpha) := \exp\left(2\pi i \operatorname{tr}(\operatorname{Res}\alpha)/p\right), \tag{2.2}$$

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 2.1 ([11, 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* $N, Q \in \mathcal{R}$ *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 (6) of Lemma 2.1 is a very simple Weyl Sum. We define a general Weyl Sum by

$$S(\alpha, \mathcal{M}, \varphi) := \sum_{A\in\mathcal{M}} E(\alpha\varphi(A)), \tag{2.3}$$

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 [11]. It reads as follows

Theorem ([11, 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*

$$S(\alpha, \mathcal{P}_n, h) \ll q^{n\left(1-\frac{1}{2^{k-1}}+\varepsilon\right)}. \tag{2.4}$$

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 [1] could prove the following result (see Hayes [9] for the case $k = 1$).

Theorem ([1, 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* $\deg H \in \{2kr, \dots, kn - 2kr\}$*. 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 paper we are interested in estimating exponential sums over polynomials that satisfy certain congruences involving Q_i-additive functions. Throughout the paper for $i = 1, \dots, r$ let f_i denote a Q_i-additive function where $Q_i \in \mathcal{R}$ are pairwise coprime polynomials and $d_i := \deg Q_i$. Furthermore let $M_i \in \mathcal{R}$ and $m_i = \deg M_i$ for $i = 1, \dots, r$. Then we define

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

moreover, let

$$\mathcal{C}(\mathbf{f}, \mathbf{J}, \mathbf{M}) = \mathcal{C}(\mathbf{J}) := \bigcup_{n\ge 1} \mathcal{C}_n(\mathbf{J}). \tag{2.5}$$

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 $\{0,1,\dots,q-1\}$ 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 $\le$ from $\mathbb{N}$ to $\mathcal{R}$ via τ such that for $A,B\in\mathcal{R}$

$$A\le B :\Leftrightarrow \tau(A)\le\tau(B). \tag{2.6}$$

By this we get a sequence $\{Z_\ell\}_{\ell\ge0}$ with $Z_\ell=\tau^{-1}(\ell)$ for all $\ell\in\mathbb{N}$. In the same way we get a sequence $\{W_\ell\}_{\ell\ge0}$ 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 $\{Z_\ell\}_{\ell\ge0}$ and $\{W_\ell\}_{\ell\ge0}$ are two rising sequences over $\mathcal{R}$ and $\mathcal{C}(\mathbf{J})$ (a sequence $\theta=\{A_\ell\}_{\ell\ge0}$ of elements in $\mathcal{R}$ is called *rising* if $i<j\Rightarrow\deg A_i\le\deg A_j$, *cf.* Hodges [10]). Finally we denote by $n_1,n_2,\dots$ positive integers such that

$$\ell-1=\deg(W_{n_\ell-1})<\deg(W_{n_\ell})=\ell. \tag{2.7}$$

With this definition we have that

$$\mathcal{P}_s=\{Z_\ell : 0\le\ell<q^s\},$$
$$\mathcal{C}_s(\mathbf{J})=\{W_\ell : 0\le\ell<n_s\}.$$

Now we are ready to state our main results. Let φ be a function. Then the difference operator Δ_ℓ ($\ell\ge0$) is recursively defined by

$$\Delta_0(\varphi(A)):=\varphi(A),$$
$$\Delta_{\ell+1}(\varphi(A);D_1,\dots,D_{\ell+1}):=\Delta_\ell(\varphi(A+D_{\ell+1});D_1,\dots,D_\ell)-\Delta_\ell(\varphi(A);D_1,\dots,D_\ell).$$

Theorem 2.2. *Let $Q_1,\dots,Q_r\in\mathcal{R}$ be relatively prime with $d_i:=\deg Q_i$ be given 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 $\mathbf{R}\in\mathcal{P}_{m_1}\times\cdots\times\mathcal{P}_{m_r}$. 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

$$E\left(\sum_{i=1}^r\frac{R_i}{M_i}\Delta_k(f_i(A);\mathbf{H})\right)\ne1,$$

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 $|\Phi_{i,k}(\mathbf{H};d_i)|\in(0,1)$.

We will use this result to prove the following theorem on uniform distribution in $\mathcal{R}$.

Theorem 2.3. *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 $M_1,\dots,M_r,J_1,\dots,J_r\in\mathcal{R}$. Let $\{W_i\}_{i\ge1}$ be the elements of the set $\mathcal{C}(\mathbf{f},\mathbf{J},\mathbf{M})$ defined in (2.5) ordered by the relation induced by τ in (2.6) and $h(Y)=\alpha_kY^k+\cdots+\alpha_1Y+\alpha_0\in\mathcal{K}_\infty[Y]$ 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.*

3. Higher Correlation

The present and the next section are devoted to the proof of Theorem 2.2. Despite some parts of the proof contain similar ideas as the proof of the rational analogue of these results (*cf.* Thuswaldner and Tichy [13, 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 generalisation of a result of Drmota and Gutenbrunner [6, Proposition 3.1]. In particular, [6] 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 $M_1, \dots, M_r \in \mathcal{R}$ are polynomials with $m_i := \deg M_i$ for $i = 1, \dots, r$.

We fix a $\mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}$ and define for $\mathbf{H} \in \mathcal{R}^k$

$$\begin{aligned} g_{\mathbf{R}_i,i,k}(A;\mathbf{H}) = g_{i,k}(A;\mathbf{H}) &:= E\left(\frac{R_i}{M_i}\Delta_k(f_i(A);\mathbf{H})\right), \\ g_{\mathbf{R},k}(A;\mathbf{H}) = g_k(A;\mathbf{H}) &:= \prod_{i=1}^{r} g_{i,k}(A;\mathbf{H}). \end{aligned} \tag{3.1}$$

We will omit the $\mathbf{R}$ (resp. the $\mathbf{R}_i$) in the index of g if this omission conserns no confusion.

We define the following correlation functions.

$$\Phi_{i,k}(\mathbf{H};n) := n^{-1}\sum_{\ell=0}^{n-1} g_{i,k}(Z_\ell;\mathbf{H}), \tag{3.2}$$

$$\Psi_{i,k}(\mathbf{h};n) := q^{-\sum_{j=1}^{k} h_j} \sum_{H_1 \in \mathcal{P}_{h_1}} \cdots \sum_{H_k \in \mathcal{P}_{h_k}} \left|\Phi_{i,k}(\mathbf{H};n)\right|^2. \tag{3.3}$$

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 3.1. *Let $h_1, \dots, h_k, n$ be positive integers. Let $d = [d_1, \dots, d_r]$ 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 $i \in \{1, \dots, r\}$ and an $\mathbf{H} \in \mathcal{P}_{d_i}^k$ such that $|\Phi_{i,k}(\mathbf{H};d_i)| < 1$ and

$$\Psi_k(\mathbf{h};n) \ll \exp\left(-\min\left\{h_1, \dots, h_k, \left\lfloor \frac{\log n}{2\log q}\right\rfloor\right\} \frac{1-\left|\Phi_{i,k}(\mathbf{H};d_i)\right|^2}{dq^{d_i}}\right) + n^{-\frac{1}{2}},$$

In order to show the uniform distribution result mentioned in the introduction we need the following adaption of [6, Proposition 1].

Proposition 3.2. *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 componentwise addition. This group we denote by

$$\mathcal{G} := \{\mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r} : g_{\mathbf{R},0}(A) = 0 \quad \forall A \in \mathcal{R}\}. \tag{3.4}$$

In order to prove Propositions 3.1 and 3.2 we start with a very special setting and continue by succesively relaxing our prerequesites. Thus the first estimation is for the special case $r = 1$ (see [6, Lemma 3.4] which contains the case $a = 1, k = 1$ of this result).

Lemma 3.3. *Let $h_1, \dots, h_k, a, n$ be positive integers. Fix $i \in \{1, \dots, r\}$. If there exists an $\mathbf{H} \in \mathcal{P}_{d_i}^k$ such that $|\Phi_{i,k}(\mathbf{H}; d_i)| < 1$ then*

$$\Psi_{i,k}(\mathbf{h}; aq^n) \ll \exp\left(-\min(h_1, \dots, h_k, n)\, \frac{1 - \left|\Phi_{i,k}(\mathbf{H}; q^{d_i})\right|^2}{d_i q^{d_i}}\right).$$

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 $\sigma_0, \sigma_1, \dots$ 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.

$$\begin{aligned} Z_{\sigma_0(y)} &= Z_y \quad 0 \le y < q^d, \\ Z_{\sigma_t(xq^d+y)} &= Z_{\sigma_t(xq^d)} \quad 0 \le y < q^d, 0 < t, \\ \{Z_{\sigma_t(\ell)} : q^{dt} \le \ell < q^{d(t+1)}\} &= \{Z_\ell : 0 \le \ell < q^d\}. \end{aligned} \tag{3.5}$$

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 $n \ge dt$.

We set

$$s = \frac{\min(h_1, \dots, h_k, n)}{d} \tag{3.6}$$

and show that for $0 \le t < s$, $P_j \in \mathcal{R}$ and $R_j \in \mathcal{P}_d$ $(j = 1, \dots, k)$

$$\Phi^{(t)}(\mathbf{P}Q + \mathbf{R}; aq^n) = \Phi^{(t+1)}(\mathbf{P}; aq^n)\Phi(\mathbf{R}; q^d) \tag{3.7}$$

holds.

As f is Q-additive we get that $f(P_jQ+R_j)=f(P_j)+f(R_j)$ for $j=1,\dots,k$. 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 (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 $\min(h_1,\dots,h_k)\geq d$

$$\Psi^{(t)}(\mathbf{h};aq^n)=\Psi^{(t+1)}(\mathbf{h}-d;aq^n)\Psi(d,\dots,d;q^d),$$

where $\mathbf{h}-d:=(h_1-d,\dots,h_k-d)$.

Thus, using (3.7), we derive

$$\begin{aligned}
&q^{\sum_{j=1}^k h_j}\Psi^{(t)}(\mathbf{h};aq^n)\\
&\quad=\sum_{P_1\in\mathcal{P}_{h_1-d}}\sum_{R_1\in\mathcal{P}_d}\cdots\sum_{P_k\in\mathcal{P}_{h_k-d}}\sum_{R_k\in\mathcal{P}_d}\overline{\Phi^{(t)}(\mathbf{P}Q+\mathbf{R};aq^n)}\Phi^{(t)}(\mathbf{P}Q+\mathbf{R};aq^n)\\
&\quad=\sum_{P_1\in\mathcal{P}_{h_1-d}}\sum_{R_1\in\mathcal{P}_d}\cdots\sum_{P_k\in\mathcal{P}_{h_k-d}}\sum_{R_k\in\mathcal{P}_d}\overline{\Phi^{(t+1)}(\mathbf{P};aq^n)\Phi(\mathbf{R};q^d)}\Phi^{(t+1)}(\mathbf{P};aq^n)\Phi(\mathbf{R};q^d)\\
&\quad=\sum_{P_1\in\mathcal{P}_{h_1-d}}\cdots\sum_{P_k\in\mathcal{P}_{h_k-d}}\overline{\Phi^{(t+1)}(\mathbf{P};aq^n)}\Phi^{(t+1)}(\mathbf{P};aq^n)\sum_{R_1\in\mathcal{P}_d}\cdots\sum_{R_k\in\mathcal{P}_d}\overline{\Phi(\mathbf{R};q^d)}\Phi(\mathbf{R};q^d)\\
&\quad=q^{\sum_{j=1}^k h_j-kd}\Psi^{(t+1)}(\mathbf{h}-d;aq^n)q^{kd}\Psi(d,\dots,d;q^d).
\end{aligned}$$

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 (3.6) we get (note that $\Psi=\Psi^{(0)}$)

$$\Psi(\mathbf{h};aq^n)=\Psi^{(0)}(\mathbf{h};aq^n)=\Psi^{(s)}(\mathbf{h}-sd;aq^n)\Psi(d,\dots,d;q^d)^s.$$

Since $\left|\Psi^{(s)}(\mathbf{h}-sd;aq^n)\right|\leq 1$ this implies that $|\Psi(\mathbf{h};aq^n)|\leq\left|\Psi(d,\dots,d;q^d)\right|^s$. Therefore we are left with estimating $\left|\Psi(d,\dots,d;q^d)\right|$. By hypothesis there exists an $\mathbf{H}\in\mathcal{P}_d^k$ with $\left|\Phi(\mathbf{H};q^d)\right|<1$, yielding

$$\Psi(d,\dots,d;q^d)\leq 1-\frac{1-\left|\Phi(\mathbf{H};q^d)\right|^2}{q^d}\ll\exp\left(-\frac{1-\left|\Phi(\mathbf{H};q^d)\right|^2}{q^d}\right).$$

Finally for given $\mathbf{h}$ and n we get that

$$|\Psi(\mathbf{h};aq^n)|\leq\left|\Psi(d,\dots,d;q^d)\right|^s\ll\exp\left(-\min(h_1,\dots,h_k,n)\,\frac{1-\left|\Phi(\mathbf{H};q^d)\right|^2}{dq^d}\right)$$

and the lemma is proven. □

Remark 3.4. As in [6, p.133] we see that $|\Phi_{i,k}(\mathbf{H};d_i)|=1$ is uncommon. Indeed, we get

$$\begin{aligned}
&\forall \mathbf{H}\in\mathcal{P}_{d_i}^k : |\Phi_{i,k}(\mathbf{H};d_i)|=1\\
&\quad\Leftrightarrow \forall \mathbf{H}\in\mathcal{P}_{d_i}^k\ \forall A\in\mathcal{P}_{d_i} : g_{i,k}(A;\mathbf{H}) \text{ is constant}\\
&\quad\Leftrightarrow \forall \mathbf{H}\in\mathcal{P}_{d_i}^k\ \forall A,B\in\mathcal{P}_{d_i} :\\
&\qquad \overline{g_{i,k-1}(A;\mathbf{H})}g_{i,k-1}(A+H_k;\mathbf{H})=\overline{g_{i,k-1}(B;\mathbf{H})}g_{i,k-1}(B+H_k;\mathbf{H})\\
&\quad\Leftrightarrow \forall \mathbf{H}\in\mathcal{P}_{d_i}^{k-1}\ \forall A,B\in\mathcal{P}_{d_i} : g_{i,k-1}(A+B;\mathbf{H})=g_{i,k-1}(A;\mathbf{H})g_{i,k-1}(B;\mathbf{H})\\
&\quad\Leftrightarrow \forall A,B\in\mathcal{P}_{d_i} : g_{i,0}(A+B)=g_{i,0}(A)g_{i,0}(B).
\end{aligned}$$

Thus

$$\begin{gathered}
\exists \mathbf{H}\in\mathcal{P}_{d}^k : |\Phi_{i,k}(\mathbf{H};d)|<1\\
\Longleftrightarrow\\
\exists A,B\in\mathcal{P}_{d_i} : g_{i,0}(A+B)\neq g_{i,0}(A)g_{i,0}(B).
\end{gathered}$$

Before we generalize Lemma 3.3 to $r>1$ we need a preliminary lemma.

Lemma 3.5 ([6, 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 [6, Lemma 3.5] for a special case of this result).

Lemma 3.6. *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 $i=1,\dots,r$ then*

$$\Psi_k(\mathbf{h};aq^n)\ll \exp\left(-\min\{h_1,\dots,h_k,n\}\frac{1-|\Phi_{i,k}(\mathbf{H};d_i)|^2}{d_iq^{d_i}}\right).$$

Proof. We fix an $\mathbf{R}\in\mathcal{P}_{m_1}\times\cdots\times\mathcal{P}_{m_r}$. Let $\ell\in\{1,\dots,r\}$ 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 ($i\in\{1,\dots,r\}$) 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 $B_1,\dots,B_r$.

Thus for a given $\mathbf{S}\in\mathcal{P}_{b_1}\times\cdots\times\mathcal{P}_{b_r}$ we define

$$N_{\mathbf{S}}:=\{Z_\ell : 0\le\ell<aq^n, Z_\ell\equiv S_1 \bmod B_1,\dots,Z_\ell\equiv S_r \bmod B_r\}.$$

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 3.5 and get

$$\begin{aligned}
aq^n\Phi_k(\mathbf{H};n)&=\sum_{A\in\mathcal{P}_n} g_k(A;\mathbf{H})\\
&=\sum_{\mathbf{S}\in\mathcal{P}_{b_1}\times\cdots\times\mathcal{P}_{b_r}}\sum_{A\in N_{\mathbf{S}}}\prod_{i=1}^r g_{i,k}(S_i;\mathbf{H})\\
&=\sum_{\mathbf{S}\in\mathcal{P}_{b_1}\times\cdots\times\mathcal{P}_{b_r}}\prod_{i=1}^r g_{i,k}(S_i;\mathbf{H})\frac{aq^n}{\prod_{j=1}^r q^{b_j}}\\
&=aq^n\prod_{i=1}^r q^{-b_i}\sum_{S_i\in\mathcal{P}_{b_i}} g_{i,k}(S_i;\mathbf{H})\\
&=aq^n\prod_{i=1}^r \Phi_{i,k}(\mathbf{H};q^{b_i}).
\end{aligned}$$

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 3.3 that

$$\Psi_k(\mathbf{h}; aq^n) \leq \Psi_{\ell,k}(\mathbf{h}; q^{b_\ell}) \ll \exp\left(-\min\{h_1, \dots, h_k, n\} \frac{1 - \left|\Phi_{\ell,k}(\mathbf{H}; q^{d_\ell})\right|^2}{d_\ell q^{d_\ell}}\right).$$

□

Finally we generalize Lemma 3.6 by allowing an arbitrary integer as second argument for Ψ_k.

Lemma 3.7. *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 $d := [d_1, \dots, d_r]$ 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 $i = 1, \dots r$, then*

$$\Psi_k(\mathbf{h}; n) \ll \exp\left(-\min\left\{h_1, \dots, h_k, \left\lfloor \frac{\log n}{2 \log q} \right\rfloor\right\} \frac{1 - |\Phi_{i,k}(\mathbf{H}; d_i)|^2}{dq^{d_i}}\right).$$

Proof. We fix $\mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}$. As in Lemma 3.6 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

$$\begin{aligned} n\Phi_k(\mathbf{P}X^{ds} + \mathbf{R}; n) &= \sum_{\ell=0}^{aq^{ds}-1} g_k(Z_\ell; \mathbf{P}X^{ds} + \mathbf{R}) + \sum_{\ell=aq^{ds}}^{aq^{ds}+b-1} g_k(Z_\ell; \mathbf{P}X^{ds} + \mathbf{R}) \\ &= aq^{ds}\Phi_k(\mathbf{P}X^{ds} + \mathbf{R}; aq^{ds}) + \sum_{y=0}^{b-1} g_k(Z_a X^{ds} + Z_y; \mathbf{P}X^{ds} + \mathbf{R}) \\ &= aq^{ds}\Phi_k(\mathbf{P}X^{ds} + \mathbf{R}; aq^{ds}) + c_a(\mathbf{P})\, b\Phi_k(\mathbf{R}; b). \end{aligned}$$

Now we show that by skipping the summands corresponding to b we do not lose to much.

$$\begin{aligned} &\left|\Phi_k(\mathbf{P}X^{ds} + \mathbf{R}; n) - \Phi_k(\mathbf{P}X^{ds} + \mathbf{R}; aq^{ds})\right| \\ &= \left|\frac{aq^{ds}\Phi_k(\mathbf{P}X^{ds} + \mathbf{R}; aq^{ds}) + c_a(\mathbf{P})\, b\Phi_k(\mathbf{R}; b)}{n} - \Phi_k(\mathbf{P}X^{ds} + \mathbf{R}; aq^{ds})\right| \\ &= \frac{b}{n}\left|c_a(\mathbf{P})\Phi_k(\mathbf{R}; b) - \Phi_k(\mathbf{P}X^{ds} + \mathbf{R}; aq^{ds})\right| \\ &\ll \frac{b}{n} \ll n^{-\frac{1}{2}}. \end{aligned}$$

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 3.6 to $\Psi_k(\mathbf{h}; aq^{ds})$ and get for fixed $\mathbf{h}$

$$\Psi(\mathbf{h}; n) \ll \exp\left(-\min\left(h_1, \dots, h_k, \frac{\log n}{2 \log q}\right) \frac{1 - \left|\Phi(\mathbf{H}; q^{d_\ell})\right|^2}{dq^{d_\ell}}\right) + n^{-\frac{1}{2}}.$$

□

Now we are ready to state the proof of the higher correlation result.

Proof of Proposition 3.1. By the assumptions of Lemma 3.7 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 3.6.

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 3.3 that $g_{i,k}(A + B; \mathbf{H}) = g_{i,k}(A; \mathbf{H}) g_{i,k}(B; \mathbf{H})$ and consequently

$$g_k(A + B; \mathbf{H}) = g_k(A; \mathbf{H}) g_k(B; \mathbf{H}) \tag{3.8}$$

for any $A, B \in \mathcal{P}_d$ and thus by the Q_i-additivity of the f_i $(i = 1, \dots, r)$ 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 [6, p.136]. □

Finally we are left to show Proposition 3.2. To this matter we state first the Weyl-van der Corput inequality in $\mathcal{K}_\infty$.

Lemma 3.8 ([5, 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 3.2. 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 3.8 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 3.1 to estimate $\Psi_1(s; n)$ and by noting that $s \to \infty$ with $n \to \infty$ the proposition follows. □

4. Weyl's Lemma for Q-additive functions

In this section we prove Theorem 2.2. Therefore we have to estimate sums of the form

$$S_n(\varphi) := \sum_{\ell=0}^{n-1} E(\varphi(Z_\ell)), \tag{4.1}$$

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 3.8, we generalise this result to the case of the kth difference operator.

Lemma 4.1. *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 $q^{s_j} \le n$ for $j = 1, \dots, k$. Further let a_j and b_j be positive integers for $j = 1, \dots, k$ such that $n = a_j q^{s_j} + b_j$ and $0 \le b_j < q^{s_j}$. Then*

$$|S_n(\varphi)|^{2^k} \le \left(\prod_{j=1}^{k} \frac{(n+q^{s_j}-b_j)^{2^{k-j}}}{q^{s_j}} \right) \sum_{P_1 \in \mathcal{P}_{s_1}} \cdots \sum_{P_k \in \mathcal{P}_{s_k}} \sum_{\ell=0}^{n-1} E(\Delta_k(\varphi(Z_\ell); P_1, \dots, P_k))$$

holds, where $u(B) = 0$ if $\tau(B) \ge n$.

Proof. We show this by induction on k. For $k = 1$ this is Lemma 3.8 with $u(Z_\ell) := E(\varphi(Z_\ell))$ for $0 \le \ell < n$.

For $k > 1$ we square the induction hypotheses and apply Cauchy's inequality to get

$$\begin{aligned} |S_n(\varphi)|^{2^{k+1}} &\le \left(\prod_{j=1}^{k} \frac{(n+q^{s_j}-b_j)^{2^{k+1-j}}}{q^{2s_j}} \right) \left| \sum_{P_1 \in \mathcal{P}_{s_1}} \cdots \sum_{P_k \in \mathcal{P}_{s_k}} \sum_{\ell=0}^{n-1} E(\Delta_k(\varphi(Z_\ell); P_1, \dots, P_k)) \right|^2 \\ &\le \prod_{j=1}^{k} \frac{(n+q^{s_j}-b_j)^{2^{k+1-j}}}{q^{s_j}} \sum_{P_1 \in \mathcal{P}_{s_1}} \cdots \sum_{P_k \in \mathcal{P}_{s_k}} \left| \sum_{\ell=0}^{n-1} E(\Delta_k(\varphi(Z_\ell); P_1, \dots, P_k)) \right|^2. \end{aligned}$$

Applying Lemma 3.8 with $u(Z_\ell) := E(\Delta_k(\varphi(Z_\ell); P_1, \dots, P_k))$ for the innermost sum yields

$$\begin{aligned} &|S_n(\varphi)|^{2^{k+1}} \\ &\quad \le \left(\prod_{j=1}^{k+1} \frac{(n+q^{s_j}-b_j)^{2^{k+1-j}}}{q^{s_j}} \right) \sum_{P_1 \in \mathcal{P}_{s_1}} \cdots \sum_{P_{k+1} \in \mathcal{P}_{s_{k+1}}} \sum_{\ell=0}^{n-1} E(\Delta_{k+1}(\varphi(Z_\ell); P_1, \dots, P_{k+1})). \end{aligned}$$

Thus the Lemma is proven. □

Now we are ready to prove Theorem 2.2.

Proof of Theorem 2.2. We want to apply our results on higher correlation in Proposition 3.1 together with the generalized Weyl inequality of Lemma 3.7. For the case that we have the expetional setting described in case 1 of Proposition 3.1. In the following section we will consider the resulting sums in the proof of Theorem 2.3.

Before we start we write for short ($h \in \mathcal{K}_\infty[Y]$)

$$S_n(h) := \sum_{\ell=0}^{n-1} E\left(h(Z_\ell) + \sum_{i=1}^{r} \frac{R_i}{M_i} f_i(Z_\ell) \right), \tag{4.2}$$

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

$$\varphi(A) = h(A) + \sum_{i=1}^{r} \frac{R_i}{M_i} f_i(A). \tag{4.3}$$

Then an application of Lemma 4.1 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 (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 3.7 to estimate $\Psi_k(s,\dots,s;n)$. Thus

$$|S_n(h)|^{2^{k+1}} \ll \frac{n^{2^{k+1}-2}}{n^{\frac{k}{2}}}\left(\exp\left(-\left\lfloor\frac{\log n}{2\log q}\right\rfloor\frac{1-|\Phi_{i,k}(\mathbf{H};d_i)|^2}{dq^{d_i}}\right)+n^{-\frac12}\right)$$

and therefore

$$S_n(h) \ll n^{1-2^{-k-1}\gamma} + n^{1-2^{-k-1}\left(\frac{k+5}{2}\right)},$$

where

$$\gamma = 2+\frac{k}{2}+\frac{1-|\Phi_{i,k}(\mathbf{H};d_i)|^2}{dq^{d_i}}.$$

□

5. Uniform Distribution

In this section we want to apply Theorem 2.2 in order to show that sequences of the form $\{h(W_\ell)\}_{\ell\ge0}$ 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 [12] or Drmota and Tichy [7] for a complete survey on that topic. In this paper we mainly follow Carlitz [3] and Dijksma [4, 5]. Further investigations on that topic have been done by Car [2] (for k-th roots) and Webb [14] (for an integral form of uniform distribution).

Let $\theta=\{A_i\}_{i\ge1}$ be a sequence of elements in $\mathcal{K}_\infty$. By $\mathcal{N}_k(N,\beta)$ we denote the number of elements A_i with $1\le i\le N$ and $\deg(A_i-\beta)<-k$. Thus

$$\mathcal{N}_k(N,\beta) := \#\{1\le i\le N : \deg(A_i-\beta)<-k\}.$$

Then we call θ uniformly distributed (according to Carlitz) in $\mathcal{K}_\infty$ if

$$\lim_{N\to\infty}\frac{1}{N}\mathcal{N}_k(N,\beta) = q^{-k} \tag{5.1}$$

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 2. First we state the Weyl Criterion for uniformly distributed sequences in $\mathcal{K}_\infty$.

Lemma 5.1 ([3, 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 $0 \neq H \in \mathcal{R}$.

Furthermore 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

$$\mathcal{J} := \{(f_1(A) \bmod M_1, \dots, f_r(A) \bmod M_r) : A \in \mathcal{R}\}$$

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 5.2. *For every $\mathbf{R} \in \mathcal{P}_{m_1} \times \cdots \times \mathcal{P}_{m_r}$ we have*

$$\lim_{n\to\infty} \frac{1}{n} |\{A \leq Z_{n-1} : f_1(A) \equiv J_1 \bmod M_1, \dots, f_r(A) \equiv J_r \bmod M_r\}| = \frac{1}{|\mathcal{J}|}.$$

This is a slight generalization of [6, Theorem 1]. The proof, however, is almost the same and we omit it.

Before we state proof of Theorem 2.3 we need a lemma which provides us with a tool to rewrite a sum over W_ℓ into one over Z_ℓ. Recall that $n_1, n_2, \dots$ are the quantities defined in (2.7).

Lemma 5.3. *Let m be a positive integer and $\varphi : \mathcal{R} \to \mathcal{K}_\infty$ be a function. Then for $n_{s-1} \leq m < n_s$ 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

$$m \sim \frac{n}{|\mathcal{J}|} \tag{5.2}$$

and if $m = n_s$ then $n = q^s$.

Proof. The trick we use to rewrite this sum goes back to Gelfond [8]. 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

$$\begin{aligned}
&\sum_{R_1\in\mathcal{P}_{m_1}} \cdots \sum_{R_r\in\mathcal{P}_{m_r}} E\left(-\sum_{i=1}^{r} \frac{R_i\,J_i}{M_i}\right) H_n(\varphi, \mathbf{R}) \\
&\quad = \sum_{R_1\in\mathcal{P}_{m_1}} \cdots \sum_{R_r\in\mathcal{P}_{m_r}} \sum_{\ell=0}^{n-1} E\left(\sum_{i=1}^{r} \frac{R_i}{M_i}(f_i(Z_\ell) - J_i)\right) E(\varphi(Z_\ell)) \\
&\quad = q^{\sum_{i=1}^{r} m_i} \sum_{\ell=0}^{m-1} E(\varphi(W_\ell)).
\end{aligned}$$

Finally we are left with estimating m. An application of Proposition 5.2 gives (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 2.3 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 [4].

Lemma 5.4 ([4, 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 $\{f(Z_\ell)\}_{\ell\geq 0}$ 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 2.3.

Proof of Theorem 2.3. We want to use Weyl's Criterion (Lemma 5.1) 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 $0\neq H\in\mathcal{R}$.

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 5.3 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 (3.4). Thus we get

$$S_m(H)=S_0+S_1,$$

where

$$S_0=\sum_{\boldsymbol{R}\in\mathcal{G}}E\left(-\sum_{i=1}^{r}\frac{R_i}{M_i}J_i\right)\sum_{\ell=0}^{n-1}E\left(\widetilde{h}(Z_\ell)\right),\tag{5.3}$$

$$S_1=\sum_{\boldsymbol{R}\in\mathcal{G}_1}\sum_{\ell=0}^{n-1}E\left(\widetilde{h}(Z_\ell)+\sum_{i=1}^{r}\frac{R_i}{M_i}(f_i(Z_\ell)-J_i)\right).\tag{5.4}$$

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 5.4 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 2.2 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 (5.2) 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 5.1 that the sequence is uniformly distributed. □

References

[1] M. Car, *Sommes de carrés de polynômes irréductibles dans* $\mathbf{F}_q[X]$, Acta Arith. **44** (1984), no. 4, 307–321.

[2] ———, *Répartition modulo* 1 *dans un corps de séries formelles sur un corps fini*, Acta Arith. **69** (1995), no. 3, 229–242.

[3] L. Carlitz, *Diophantine approximation in fields of characteristic p*, Trans. Amer. Math. Soc. **72** (1952), 187–208.

[4] 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.

[5] ———, *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.

[6] 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.

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

[8] A. O. Gel′fond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*, Acta Arith. **13** (1967/1968), 259–265.

[9] D. R. Hayes, *The expression of a polynomial as a sum of three irreducibles*, Acta Arith. **11** (1966), 461–488.

[10] J. H. Hodges, *Uniform distribution of sequences in* GF$[q, x]$, Acta Arith **12** (1966/1967), 55–75.

[11] R. M. Kubota, *Waring's problem for* $\mathbf{F}_q[x]$, Dissertationes Math. (Rozprawy Mat.) **117** (1974), 60.

[12] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Interscience [John Wiley & Sons], New York, 1974, Pure and Applied Mathematics.

[13] J. M. Thuswaldner and R. F. Tichy, *Waring's problem with digital restrictions*, Israel J. Math. **149** (2005), 317–344, Probability in mathematics.

[14] W. A. Webb, *Uniformly distributed functions in* GF$[q, x]$ *and* GF$\{q, x\}$, Ann. Mat. Pura Appl. (4) **95** (1973), 285–291.

(M.G. Madritsch) Department of Mathematics and Information Technology, University of Leoben, A-8700 Leoben, Austria

E-mail address: Manfred.Madritsch@mu-leoben.at

(J.M. Thuswaldner) Department of Mathematics and Information Technology, University of Leoben, A-8700 Leoben, Austria

E-mail address: Joerg.Thuswaldner@mu-leoben.at