WARING'S PROBLEM WITH DIGITAL RESTRICTIONS

JÖRG M. THUSWALDNER AND ROBERT F. TICHY

Dedicated to Professor Hillel Furstenberg

Abstract. The aim of this paper is to consider an analogue of Waring's problem with digital restrictions. In particular, we prove the following result. Let $s_q(n)$ be the q-adic sum of digits function and let h, m be fixed positive integers. Then for $s > 2^k$ there exists $n_0 \in \mathbb{N}$ such that each integer $n \geq n_0$ has a representation of the form

$$n = x_1^k + \cdots + x_s^k \quad \text{where} \quad s_q(x_i) \equiv h(m).$$

We will even give an asymptotic formula for the number of representations of n in this way. The result is shown with help of the circle method in combination with a "digital" version of Weyl's Lemma.

1. Notation

As usual, $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ and $\mathbb{C}$ denote the set of positive integers, integers, real and complex numbers, respectively. The abbreviation $e(x) := \exp(2\pi i x)$ will be used, $\lfloor x \rfloor$ is the greatest integer less than or equal to $x \in \mathbb{R}$. Furthermore, we will write $\lceil x \rceil$ for the smallest integer greater than or equal to x. For the cardinality of a set $\mathcal{S}$ we will write $|\mathcal{S}|$. Vectors will be written in bold face. Concerning the indices of the elements of a vector we will use the conventions

$$\mathbf{r} := (r_1, \ldots, r_k) \quad \text{and} \quad \mathbf{r}_j := (r_{j1}, \ldots, r_{jk}).$$

We will use the notations $f(x) = \mathcal{O}(g(x))$ as well as $f(x) \ll g(x)$ to express that $f(x) < cg(x)$ for some constant c and all sufficiently large $x \in \mathbb{R}$. If the implied constant c depends on a certain parameter, say ε, this will be either mentioned explicitly or indicated by $f(x) \ll_\varepsilon g(x)$.

If $I := \{n \in \mathbb{Z} \mid a \leq n < b\}$ is an *interval of integers* then we use the abbreviation

$$cI := \{n \in \mathbb{Z} \mid ca \leq n < cb\} \tag{1}$$

for $c \in \mathbb{N}$.

Date: January 12, 2004.

Key words and phrases. Waring's problem, Weyl sum, circle method, digital sum, correlation.

The first author was supported by the Austrian Science Foundation project S8310.

The second author was supported by the Austrian Science Foundation project S8308.

2. Introduction

Let $A \subseteq \mathbb{N}$ and $s \in \mathbb{N}$. If each positive integer $N \in \mathbb{N}$ admits a representation of the form

$$N = x_1 + \cdots + x_s \quad \text{with} \quad x_1, \ldots, x_s \in A \tag{2}$$

we say that A is a *basis* of $\mathbb{N}$ of order s. If a representation of the shape (2) only exists if N is sufficiently large we call A an *asymptotic basis* of $\mathbb{N}$ of order s (cf. for instance Nathanson [18]).

It is a fundamental problem in additive number theory to decide whether a given set $A \subseteq \mathbb{N}$ is a basis (resp. asymptotic basis) or not (cf. Hua [14], Nathanson [18, 19], Vinogradov [30]). If A turns out to be a basis one is interested to find its smallest possible order. We mention Goldbach's problem, where A is taken to be the set of primes or Waring's problem which corresponds to

$$A = A_k := \{n^k \mid n \in \mathbb{N}\} \quad (k \in \mathbb{N} \text{ fixed}).$$

We use the common notations $g(k)$ and $G(k)$ for the smallest possible number s such that A_k is a basis or asymptotic basis of order s, respectively. The best known bound for $G(k)$ is due to Wooley [31] and reads

$$G(k) \le k(\log k + \log\log k + \mathcal{O}(1)).$$

For results on $g(k)$ we refer the reader to Vaughan [25, p. 1f]. Hardy and Littlewood were the first to give an asymptotic formula (now called the Hardy-Littlewood formula) for the number of representations of a sufficiently large integer as the sum of s elements of A_k. We denote the smallest number of s for which this formula holds by $\tilde{G}(k)$ and remark that the best estimate for $\tilde{G}(k)$ is due to Ford [9] and asserts that

$$\tilde{G}(k) \le k^2(\log k + \log\log k + \mathcal{O}(1)).$$

For small values of k these results can be refined. We refer for instance to the results by Vaughan and Wooley in [26, 27, 28, 29]. The present paper is devoted to a variant of Waring's problem with digital constraints. To make this more precise let $s_q(n)$ be the q-adic sum of digits function which assigns to each positive integer n the sum

$$s_q(n) = c_0 + \cdots + c_r$$

of digits in its (unique) q-adic representation

$$n = c_0 + c_1 q + \cdots + c_r q^r.$$

With help of $s_q(n)$ we define the set

$$U_{h,m}(N) := \{n < N \mid s_q(n) \equiv h(m)\}.$$

This set has been studied for instance by Gelfond [12] and Mauduit-Sárközy [16]. Our goal is to show that each sufficiently large $N \in \mathbb{N}$ admits a representation of the shape

$$N = x_1^k + \cdots + x_s^k, \quad \text{with} \quad x_1, \ldots, x_s \in U_{h,m}(N)$$

for each fixed $s > 2^k$ if $(m, q-1) = 1$. In other words, this means that

$$A_{k,h,m} := \left\{ n^k \mid s_q(n) \equiv h(m) \right\}$$

forms an asymptotic basis of order 2^k+1. In fact, by very slight modifications we can prove even more: we get that if $s > 2^k$ then each sufficiently large $N \in \mathbb{N}$ has a representation of the shape

$$N = x_1^k + \cdots + x_s^k, \quad \text{with} \quad s_{q_i}(x_i) \equiv h_i(m_i) \quad (1 \leq i \leq s).$$

Again the condition $(m_i, q_i - 1) = 1$ is needed.

Analogously to the notation for the ordinary Waring's problem we give the following definition.

Definition 2.1. *Let $G_{h,m}(k)$ be the smallest integer s such that $A_{k,h,m}$ forms an asymptotic basis of order s of $\mathbb{N}$. Furthermore, let $g_{h,m}(k)$ be the smallest integer s such that $A_{k,h,m} \cup \{1\}$ forms a basis of order s of $\mathbb{N}$.*

Note that $\{1\}$ has to be added to $A_{k,h,m}$ in the definition of $g_{h,m}(k)$ because otherwise 1 could not have any representation.

There exist also other restricted versions of Waring's problem. One of them is the Waring's problem restricted to sums of k-th powers of primes. An account of it can be found for instance in Hua [14] (cf. also Brüdern's papers [4, 5] for a new approach to this subject). A more recent restriction of Waring's problem was investigated by Harcos [13]. Generalizing a result of Balog and Sárközy [1] he considered Waring's problem for sums of k-th powers of integers having not too large prime factors. In Brüdern-Fouvry [6] an analogue of Lagrange's four squares theorem for almost primes was shown.

The sum of digits function was the subject of many papers in the last decades. Its basic property is *q-additivity*, i.e. if $a, b, h \in \mathbb{N}$ with $b < q^h$ then

$$s_q(aq^h + b) = s_q(a) + s_q(b).$$

One of the first papers on $s_q(n)$ was Bellman-Shapiro [2] where the summatory function of $s_q(n)$ and its iterates were treated. An exact formula for the summatory function of $s_q(n)$ was later proved by Delange [7]. The distribution of $s_q(n)$ in residue classes has been studied in Gelfond [12]. More recent results on $s_q(n)$ can be found for instance in Drmota-Schoissengeier [8], Mauduit-Sárközy [16, 17] or Thuswaldner-Tichy [23]. In order to prove our results we will have to establish auto-correlation results of the sum of digits function. Special cases of these results can be found in Bésineau [3] and Kim [15], where the simultaneous distribution of sum of digits functions with respect to different bases is investigated. We have to extend these results in the present paper in order to establish a "digital" version of Weyl's Lemma. This result seems to be of interest also in its own right. We will use it in order to derive our result on Waring's problem with digital restrictions.

One could ask whether it is possible to give results on a version of Waring's problem using only k-th powers of primes with digital restrictions. However, this seems to be very hard to settle since up to now it is not even known if there exist infinitely many prime numbers whose sum of digits function satisfies a given congruence. The best known result in that direction is contained in Fouvry-Mauduit [10, 11].

In earlier papers Diophantine equations with digital restrictions have been considered. Generalizing a result of Stewart [22] on sets of numbers having small sum of digits function simultaneously in two different bases, Schlickewei [21] studied the solutions of a certain Diophantine equation having bounded sum of digits. This result has been extended further to a more general notion of number systems in Pethő-Tichy [20].

The present paper is organized as follows. In the next section we present our main results: the Hardy-Littlewood asymptotic formula for Waring's problem with digital constraints together with the generalization mentioned above (Theorem 3.1 and Theorem 3.2), a higher auto-correlation result for the sum of digits function (Theorem 3.3) and a "digital" version of Weyl's Lemma (Theorem 3.4). Sections 4, 5 and 6 contain preliminary results needed in order to prove Theorem 3.3. This result is finally proved in Section 7. Section 8 is devoted to the deduction of the variant of Weyl's Lemma from the auto-correlation result. The variant of Weyl's Lemma is finally used in Section 9, where we show that $A_{k,h,m}$ is an asymptotic basis of $\mathbb{N}$ for each triple $k,h,m \in \mathbb{N}$ and that the asymptotic formula in Theorem 3.2 holds. The proof of Theorem 3.1 turns out to run along exactly the same lines as the proof of the special case. Our main tool here is the circle method. The paper ends with a short section containing some concluding remarks.

3. Statement of the main results

We will now state our results.

Theorem 3.1. *Let $s,k \in \mathbb{N}$, and $h_i, m_i, q_i \in \mathbb{N}$ $(1 \leq i \leq s)$ with $m_i \geq 2$, $q_i \geq 2$ and $(q_i - 1, m_i) = 1$. Let $r_{k,s,h_i,m_i}(N)$ be the number of representations of N in the form*

$$N = x_1^k + \cdots + x_s^k \qquad (s_{q_i}(x_i) \equiv h_i(m_i)).$$

Then for $s > 2^k$ there exists a positive constant δ such that

$$r_{k,s,h_i,m_i}(N) \;=\; \frac{1}{m_1 \cdots m_s}\mathfrak{S}(N)\Gamma\left(1+\frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} N^{\frac{s}{k}-1} + \mathcal{O}\left(N^{\frac{s}{k}-1-\delta}\right).$$

The implied constant depends only on s, k and m_i. $\mathfrak{S}$ is an arithmetic function for which there exist positive constants $0 < c_1 < c_2$ depending only on k and s such that

$$c_1 < \mathfrak{S}(N) < c_2.$$

The following special case yields a new asymptotic basis of $\mathbb{N}$.

Theorem 3.2. *Let $s,k,h,m,q \in \mathbb{N}$ with $m \geq 2$, $q \geq 2$ and $(q-1,m) = 1$. Let $r_{k,s,h,m}(N)$ be the number of representations of N in the form*

$$N = x_1^k + \cdots + x_s^k \qquad (x_1, \ldots, x_k \in U_{h,m}(N)).$$

Then for $s > 2^k$ there exists a positive constant δ such that

$$r_{k,s,h,m}(N) = \frac{1}{m^s}\mathfrak{S}(N)\Gamma\left(1+\frac{1}{k}\right)^s \Gamma\left(\frac{s}{k}\right)^{-1} N^{\frac{s}{k}-1} + \mathcal{O}\left(N^{\frac{s}{k}-1-\delta}\right).$$

The implied constant depends only on s, k and m. $\mathfrak{S}$ is an arithmetic function for which there exist positive constants $0 < c_1 < c_2$ depending only on k and s such that

$$c_1 < \mathfrak{S}(N) < c_2.$$

This implies that $A_{k,h,m} = \{n^k \mid s_q(n) \equiv h(m)\}$ forms an asymptotic basis of order $2^k + 1$ of $\mathbb{N}$, i.e.

$$G_{h,m}(k) \leq 2^k + 1.$$

The proof of these theorems relies on the circle method and on a correlation result for the sum of digits function. Before we state this result we recall the definition of the higher difference operators Δ_j. Let φ be an arithmetic function. Then

$$\Delta_1(\varphi(x); y) := \varphi(x+y) - \varphi(x).$$

The higher difference operators are defined recursively by

$$\Delta_{j+1}(\varphi(x), y_1, \ldots, y_{j+1}) := \Delta_1(\Delta_j(\varphi(x); y_1, \ldots, y_j); y_{j+1}) \quad (j \geq 1).$$

In what follows we will use the function

$$p(k,q) := \left\lceil 2\frac{k(k+2)}{q-1} + 2k + 5 \right\rceil. \tag{3}$$

We will need the following higher correlation result for $s_q(n)$, which is a generalization of [15, Proposition 1] and which is of interest also in its own right.

Theorem 3.3. *Let k, m, h, q and N be positive integers with $m \geq 2$, $q \geq 2$ and $m \nmid h(q-1)$. Let $I_1, \ldots, I_k, J$ be intervals of integers with $\sqrt{N} \leq |I_j|, |J| \leq N$ $(1 \leq j \leq k)$. Set*

$$Y(I_1, \ldots, I_k, J) := \sum_{h_1 \in I_1} \cdots \sum_{h_k \in I_k} \left| \sum_{n \in J} e\left(\frac{h}{m}\Delta_k(s_q(n); h_1, \ldots, h_k)\right) \right|^2.$$

Then

$$Y(I_1, \ldots, I_k, J) \ll |I_1| \cdots |I_k| |J|^2 N^{-\eta}$$

holds with $\eta := \frac{1}{m^2 q^{p(k,q)}} > 0$.

This result leads to the following "digital" version of Weyl's Lemma which will be used in the proof of Theorem 3.2.

Theorem 3.4. *Let k, m, ℓ, q and N be positive integers with $m \geq 2$, $q \geq 2$ and $m \nmid \ell(q-1)$. Then the estimate*

$$\left| \sum_{n<N} e\left(\theta n^k + \frac{\ell}{m} s_q(n)\right) \right| \ll N^{1-\gamma}$$

holds uniformly in $\theta \in [0,1)$ with $\gamma := \eta 2^{-(k+1)}$. Here η is as in Theorem 3.3.

Remark 3.1. *If one does not care about its order, the assertion that $A_{k,h,m}$ forms an asymptotic basis can be proved easily in the following way.*

Suppose that the set $\mathcal{A}$ of non-negative integers has positive asymptotic density. Suppose further that for each prime p there exist numbers $a_p, b_p \in \mathcal{A}$ such that $p \mid a_p$ and $p \nmid b_p$. Then for any integer k the set $\mathcal{A}^k := \{n^k \mid n \in \mathcal{A}\}$ is an asymptotic basis. This can be shown by combining arguments about Schnirel'man density and the observation that the set of s-fold sums of elements of $\mathcal{A}^k$ has positive asymptotic density for $s \geq 2^{k-1}$. The latter follows from [24, Theorem 2]*, which implies that*

$$\begin{aligned}
&\left|\left\{n_1, \ldots, n_{2s} \in \mathcal{A}(N) \,\middle|\, n_1^k + \ldots + n_s^k = n_{s+1}^k + \ldots + n_{2s}^k\right\}\right| \\
&\qquad \leq \left|\left\{n_1, \ldots, n_{2s} < N \,\middle|\, n_1^k + \ldots + n_s^k = n_{s+1}^k + \ldots + n_{2s}^k\right\}\right| \\
&\qquad \ll N^{2s-k}
\end{aligned}$$

holds for $s \geq 2^{k-1}$. Here $\mathcal{A}(N) := \{n < N \mid n \in \mathcal{A}\}$.

It is easy to show that the choice $\mathcal{A} := \{n \mid s_q(n) \equiv h(m)\}$ fulfills the above conditions. In particular, we see from Fermat's theorem that we can define the integers a_p and b_p by choosing I and J in the expression

$$\sum_{i=0}^{I-1} q^{i(p-1)} + \sum_{j=0}^{J-1} q^{1+j(p-1)}$$

properly.

Remark 3.2. *The bound for s in Theorem 3.1 and Theorem 3.2 is surely not best possible. In order to make it smaller at least in Theorem 3.2, better estimates of the norm*

$$\int_0^1 \left|\sum_{n<N} e\left(\theta n^k + \frac{\ell}{m} s_q(n)\right)\right|^j d\theta \tag{4}$$

are needed for certain values of $j \in \mathbb{N}$. Obtaining such estimates may be doable but is certainly quite involved (a very special case of a similar integral as in (4) *has been treated in* [10]*). Furthermore, we expect that these estimates will not lead to results of the same quality as the refinements of Hua's Lemma in Waring's problem (as for instance in* [31]*).*

4. Operators on a class of discrete functions

In order to prove Theorem 3.3 we need some tricky but elementary calculations. The key step in the proof of this result is done by selecting two terms of the form $e(x)$ from a certain exponential sum and proving that the sum of these two terms has modulus less than two. In order to be able to select the proper terms we set up a class of functions together with some operators acting on it.

Consider the sets

$$\mathcal{M} := \{1, 2, \ldots, k\} \quad \text{and} \quad \mathcal{M}' := \{0, 1, 2, \ldots, k+1\}$$

and define the class of functions

$$\mathcal{F} := \{f : 2^{\mathcal{M}} \to \mathcal{M}'\}$$

(here 2^M denotes the set of all subsets of $\mathcal{M}$). Especially two elements of $\mathcal{F}$ will be important in the following discussions. These are

$$F_0(\mathcal{S}) := 0 \qquad \text{for all } \mathcal{S} \subseteq \mathcal{M}, \tag{5}$$

$$F_1(\mathcal{S}) := \begin{cases} 1 & \text{if } \mathcal{S} = \mathcal{M} \\ 0 & \text{otherwise} \end{cases}. \tag{6}$$

On $\mathcal{F}$ we want to define the operator

$$\Xi_{\mathbf{r},i}(f)(\mathcal{S}) := \left\lfloor \frac{i + \sum_{j\in\mathcal{S}} r_j + f(\mathcal{S})}{q} \right\rfloor$$

for each vector $\mathbf{r} = (r_1, \dots, r_k) \in \{0, \dots, q-1\}^k$ and each $0 \le i < q$.

Lemma 4.1. *For each pair $\mathbf{r}, i$ we have*

$$\Xi_{\mathbf{r},i}(\mathcal{F}) \subseteq \mathcal{F}.$$

Proof. We have to show that $\Xi_{\mathbf{r},i}(f)(\mathcal{S})$ always lies in $\mathcal{M}'$. Since $f \in \mathcal{F}$ and with the restrictions on $\mathbf{r}, i$ we see that

$$0 \le \left\lfloor \frac{i + \sum_{j\in\mathcal{S}} r_j + f(\mathcal{S})}{q} \right\rfloor \le \frac{(k+1)(q-1)+k+1}{q} = k+1$$

and we are done. $\square$

We will need iterates of $\Xi_{\mathbf{r},i}$. These are defined by

$$\Xi_{\{\mathbf{r}_\ell,i_\ell\}_{1\le\ell\le L}} := \Xi_{\mathbf{r}_L,i_L} \circ \cdots \circ \Xi_{\mathbf{r}_1,i_1}.$$

Dividing k by $q-1$ yields a representation

$$k = d(q-1) + \rho \qquad (0 \le \rho < q-1). \tag{7}$$

Set $L'' := \left\lfloor \frac{k-1}{q-1} \right\rfloor + 1$. If $\rho = 0$ set

$$\begin{aligned} \mathbf{v}_\ell &:= (v_{\ell 1}, \dots, v_{\ell k}) \in \mathbb{Z}^k \quad \text{with} \\ v_{\ell j} &:= \begin{cases} 1 & \text{if } j \in \{(\ell-1)(q-1)+1, \dots, \ell(q-1)\} \\ 0 & \text{otherwise} \end{cases} \qquad (1 \le \ell \le L''). \end{aligned}$$

If on the contrary $\rho > 0$ set

$$\begin{aligned} \mathbf{v}_1 &:= (\underbrace{1, \dots, 1}_{\rho \text{ times}}, 0, \dots, 0) \in \mathbb{Z}^k, \\ \mathbf{v}_\ell &:= (v_{\ell 1}, \dots, v_{\ell k}) \in \mathbb{Z}^k \quad \text{with} \\ v_{\ell j} &:= \begin{cases} 1 & \text{if } j \in \{(\ell-2)(q-1)+\rho+1, \dots, (\ell-1)(q-1)+\rho\} \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

for $2 \le \ell \le L''$.

Lemma 4.2. *The following two assertions hold:*

(i) *Let $f \in \mathcal{F}$ be arbitrary. Then*

$$\Xi_{\{\mathbf{0},0\}_{1\le \ell \le L'}}(f) = F_0$$

if $L' := \left\lfloor \frac{\log(k+1)}{\log q} \right\rfloor + 1$.

(ii) *Let*

$$\begin{aligned} i_1 &:= \begin{cases} 1, & \text{if } \rho = 0 \\ q-\rho, & \text{if } \rho > 0 \end{cases}, \\ i_\ell &:= 0 \qquad (2 \le \ell \le L'') \qquad \text{and} \\ \mathbf{r}_\ell &:= \mathbf{v}_\ell \qquad (1 \le \ell \le L''). \end{aligned}$$

Then $\Xi_{\{\mathbf{r}_\ell, i_\ell\}_{1 \le \ell \le L''}}(F_0) = F_1$.

Proof. (i) Let $f \in \mathcal{F}$ and $\mathcal{S} \subseteq \mathcal{M}$ be arbitrary. Then

$$\Xi_{\mathbf{0},0}(f)(\mathcal{S}) = \left\lfloor \frac{f(\mathcal{S})}{q} \right\rfloor \le \frac{f(\mathcal{S})}{q}.$$

Iterating L' times shows

$$\Xi_{\{\mathbf{0},0\}_{1\le \ell \le L'}}(f)(\mathcal{S}) \le \left\lfloor \frac{f(\mathcal{S})}{q^{L'}} \right\rfloor = 0$$

for all $\mathcal{S}$.

(ii) Let $\rho = 0$. The proof of the case $\rho > 0$ runs along the same lines. From the definitions of $\Xi_{\mathbf{r},i}$ and $\mathbf{v}_1$ we get

$$\begin{aligned} \Xi_{\mathbf{r}_1, i_1}(F_0)(\mathcal{S}) &= \left\lfloor \frac{1 + \left(\sum_{t \in \mathcal{S} \cap \{1,\dots,q-1\}} 1 \right)}{q} \right\rfloor \\ &= \begin{cases} 1 & \text{if } \{1,2,\dots,q-1\} \subseteq \mathcal{S} \\ 0 & \text{otherwise} \end{cases}. \end{aligned}$$

Now we proceed by induction. Suppose that

(8) $$\Xi_{\{\mathbf{r}_\ell, i_\ell\}_{1 \le \ell \le j-1}}(F_0) = \begin{cases} 1 & \text{if } \{1,\dots,(j-1)(q-1)\} \subseteq \mathcal{S} \\ 0 & \text{otherwise} \end{cases}$$

holds for some $j \leq L''$. Then, again by the definition of $\Xi_{\mathbf{r},i}$ and $\mathbf{v}_j$ we obtain that

$$\Xi_{\{\mathbf{r}_\ell,i_\ell\}_{1\leq\ell\leq j}}(F_0) = \begin{cases} \left\lfloor \frac{\left(\sum_{t\in\mathcal{S}\cap\{(j-1)(q-1)+1,\dots,j(q-1)\}} 1\right)+1}{q} \right\rfloor & \text{if } \{1,\dots,(j-1)(q-1)\}\subseteq\mathcal{S} \\ \left\lfloor \frac{\sum_{t\in\mathcal{S}\cap\{(j-1)(q-1)+1,\dots,j(q-1)\}} 1}{q} \right\rfloor & \text{otherwise} \end{cases}$$

holds. It is easy to see that this yields (8) for j instead of $j-1$. Thus by induction we get

$$\Xi_{\{\mathbf{r}_\ell,i_\ell\}_{1\leq\ell\leq L''}}(F_0) = \begin{cases} 1 & \text{if } \{1,\dots,k\}\subseteq\mathcal{S} \\ 0 & \text{otherwise} \end{cases}$$

because $L''(q-1)\geq k$. Since the only subset of $\mathcal{M}$ which has $\{1,\dots,k\}$ as a subset is $\mathcal{M}$ itself the last function is F_1 and we are done. □

5. Recurrences for auto-correlation functions of $s_q(n)$

In this section we set up a recurrence for functions related to the auto-correlation function $Y(I_1,\dots,I_k,J)$ defined in Theorem 3.3. This is done by "multiplying" all the intervals $I_1,\dots,I_k,J$ by q in the sense defined in (1) and exploiting the q-additivity of $s_q(n)$.

Let $I_1,\dots,I_k,J$ be intervals of integers. Define the following functions.

$$\begin{aligned} \Phi(h_1,\dots,h_k;J;f) &:= \sum_{n\in J} e\left(\frac{h}{m}\sum_{\mathcal{S}\subseteq\mathcal{M}}(-1)^{k-|\mathcal{S}|}s_q\left(n+\sum_{t\in\mathcal{S}}h_t+f(\mathcal{S})\right)\right), \\ \Psi(h_1,\dots,h_{k-1};I_k,J;f_1,f_2) &:= \sum_{h_k\in I_k}\Phi(h_1,\dots,h_k;J;f_1)\overline{\Phi(h_1,\dots,h_k;J;f_2)}, \qquad (9) \\ X(I_1,\dots,I_k,J;f_1,f_2) &:= \sum_{h_1\in I_1}\cdots\sum_{h_{k-1}\in I_{k-1}}\Psi(h_1,\dots,h_{k-1};I_k,J;f_1,f_2). \end{aligned}$$

Here the h_i $(1\leq i\leq k)$ are integers and $f,f_1,f_2\in\mathcal{F}$.

Note that

$$\sum_{n\in J} e\left(\frac{h}{m}\Delta_k(s_q(n);h_1,\dots,h_k)\right) = \Phi(h_1,\dots,h_k;J;F_0).$$

Thus for the sum $Y(I_1,\dots,I_k,J)$ defined in Theorem 3.3

$$Y(I_1,\dots,I_k,J) = X(I_1,\dots,I_k,J;F_0,F_0)$$

holds. We will derive estimates for $X(I_1,\dots,I_k,J;f_1,f_2)$ for each pair $f_1,f_2\in\mathcal{F}$. From this obviously follows the estimate for $Y(I_1,\dots,I_k,J)$.

In the sequel we will use for short the vectors

$$\mathbf{r} := (r_1,\dots,r_k) \quad\text{and}\quad \mathbf{h} := (h_1,\dots,h_k).$$

Proposition 5.1. *Let $f_1, f_2 \in \mathcal{F}$ and let $I_1, \dots, I_k, J$ be intervals of integers. Then*

$$\begin{aligned} X(qI_1, \dots, qI_k, qJ; f_1, f_2) &= \sum_{r_1=0}^{q-1} \cdots \sum_{r_k=0}^{q-1} \sum_{i_1=0}^{q-1} \sum_{i_2=0}^{q-1} \alpha(f_1, f_2, \mathbf{r}, i_1, i_2) \\ &\quad \times X(I_1, \dots, I_k, J; \Xi_{\mathbf{r},i_1}(f_1), \Xi_{\mathbf{r},i_2}(f_2)). \end{aligned}$$

Here

$$\alpha(f_1, f_2, \mathbf{r}, i_1, i_2) := e\left(\frac{h}{m} \sum_{\mathcal{S} \subseteq \mathcal{M}} (-1)^{k-|\mathcal{S}|} (b(f_1, \mathcal{S}, \mathbf{r}, i_1) - b(f_2, \mathcal{S}, \mathbf{r}, i_2))\right).$$

The integer $b(f, \mathcal{S}, \mathbf{r}, i) \in \{0, \dots, q-1\}$ is defined as the remainder occurring at the division of $i + \sum_{t \in \mathcal{S}} r_t + f(\mathcal{S})$ by q.

Proof. We start with the first of the functions given in (9). Note that for $1 \le r_1, \dots, r_k < q$ we have

$$\Phi(q\mathbf{h} + \mathbf{r}; qJ; f) = \sum_{i=0}^{q-1} \sum_{n \in J} e\left(\frac{h}{m} \sum_{\mathcal{S} \subseteq \mathcal{M}} (-1)^{k-|\mathcal{S}|} s_q\left(qn + \sum_{t \in \mathcal{S}} qh_t + i + \sum_{t \in \mathcal{S}} r_t + f(\mathcal{S})\right)\right). \tag{10}$$

Now, by the definition of $\Xi_{\mathbf{r},i}$ and $b(f, \mathcal{S}, \mathbf{r}, i)$ we have

$$i + \sum_{t \in \mathcal{S}} r_t + f(\mathcal{S}) = \Xi_{\mathbf{r},i}(f)(\mathcal{S})q + b(f, \mathcal{S}, \mathbf{r}, i).$$

By the q-additivity of $s_q(n)$ this implies that

$$\begin{aligned} s_q\left(qn + \sum_{t \in \mathcal{S}} qh_t + i + \sum_{t \in \mathcal{S}} r_t + f(\mathcal{S})\right) &= s_q\left(qn + \sum_{t \in \mathcal{S}} qh_t + q\Xi_{\mathbf{r},i}(f)(\mathcal{S}) + b(f, \mathcal{S}, \mathbf{r}, i)\right) \\ &= s_q\left(n + \sum_{t \in \mathcal{S}} h_t + \Xi_{\mathbf{r},i}(f)(\mathcal{S})\right) + b(f, \mathcal{S}, \mathbf{r}, i). \end{aligned}$$

Inserting this in (10) yields

$$\Phi(q\mathbf{h} + \mathbf{r}; qJ; f) = \sum_{i=0}^{q-1} e\left(\frac{h}{m} \sum_{\mathcal{S} \subseteq \mathcal{M}} (-1)^{k-|\mathcal{S}|} b(f, \mathcal{S}, \mathbf{r}, i)\right) \Phi(\mathbf{h}; J; \Xi_{\mathbf{r},i}(f)).$$

Using the definition of the auto-correlation function Ψ in (9) this immediately leads to

$$\begin{aligned} \Psi(qh_1 + r_1, \dots, qh_{k-1} + r_{k-1}; qI_k, qJ; f_1, f_2) &= \\ &\sum_{r_k=0}^{q-1} \sum_{i_1=0}^{q-1} \sum_{i_2=0}^{q-1} \alpha(f_1, f_2, \mathbf{r}, i_1, i_2) \\ &\times \Psi(h_1, \dots, h_{k-1}; I_k, J; \Xi_{\mathbf{r},i_1}(f_1), \Xi_{\mathbf{r},i_2}(f_2)). \end{aligned}$$

Summing up over $h_1, \ldots, h_{k-1}$ finally yields

$$\begin{aligned} X(qI_1, \ldots, qI_k, qJ; f_1, f_2) &= \sum_{r_1=0}^{q-1} \cdots \sum_{r_k=0}^{q-1} \sum_{i_1=0}^{q-1} \sum_{i_2=0}^{q-1} \alpha(f_1, f_2, \mathbf{r}, i_1, i_2) \\ &\quad \times X(I_1, \ldots, I_k, J; \Xi_{\mathbf{r},i_1}(f_1), \Xi_{\mathbf{r},i_2}(f_2)). \end{aligned}$$

□

In what follows we will need a more explicit representation of $\alpha(f_1, f_2, \mathbf{r}, i_1, i_2)$ for certain values of the parameters. In particular, we will show the following result.

Lemma 5.1. *Let F_0 and F_1 be as in* (5) *and* (6)*. Furthermore, let*

$$\mathbf{0} := (\underbrace{0, \ldots, 0}_{k \ \textit{times}}).$$

Then we have

$$\begin{aligned} \alpha(F_0, F_0, \mathbf{0}, 0, 0) &= e\,(0)\,, \\ \alpha(F_1, F_0, \mathbf{0}, 0, 0) &= e\left(\frac{h}{m}\right) \quad \textit{and} \\ \alpha(F_1, F_0, \mathbf{0}, q-1, 0) &= e\left(\frac{h}{m}(1-q)\right). \end{aligned}$$

Proof. Recall that

$$\alpha(f_1, f_2, \mathbf{r}, i_1, i_2) \ := \ e\left(\frac{h}{m} \sum_{\mathcal{S} \subseteq \mathcal{M}} (-1)^{k-|\mathcal{S}|} (b(f_1, \mathcal{S}, \mathbf{r}, i_1) - b(f_2, \mathcal{S}, \mathbf{r}, i_2))\right),$$

where $b(f, \mathcal{S}, \mathbf{r}, i)$ is the remainder occurring at the division of $i + \sum_{t \in \mathcal{S}} r_t + f(\mathcal{S})$ by q.

- If $f = F_0$ and all r_t as well as i is zero, this remainder has to be zero for each $\mathcal{S} \subseteq \mathcal{M}$. Thus also
$$\sum_{\mathcal{S} \subseteq \mathcal{M}} (-1)^{k-|\mathcal{S}|} b(F_0, \mathcal{S}, \mathbf{0}, 0) = 0.$$
- If $f = F_1$ and all r_t as well as i is zero, $b(F_1, \mathcal{S}, \mathbf{0}, 0) = 0$ unless $\mathcal{S} = \mathcal{M}$. In the latter case it is equal to 1. This means that
$$\sum_{\mathcal{S} \subseteq \mathcal{M}} (-1)^{k-|\mathcal{S}|} b(F_1, \mathcal{S}, \mathbf{0}, 0) = 1.$$
- If $f = F_1$, all r_t are zero and $i = q-1$, then again $b(F_1, \mathcal{S}, \mathbf{0}, q-1) = q-1$ unless $\mathcal{S} = \mathcal{M}$. For the latter case we note that
$$i + \sum_{t \in \mathcal{M}} r_t + f(\mathcal{M}) = q - 1 + 1 = q.$$

Since $q \equiv 0 (\mathrm{mod}\ q)$ we conclude that $b(F_1, \mathcal{M}, \mathbf{0}, q-1) = 0$. This implies that

$$\begin{aligned}\sum_{\mathcal{S} \subseteq \mathcal{M}} (-1)^{k-|\mathcal{S}|} b(F_1, \mathcal{S}, \mathbf{0}, q-1) &= -q + 1 + \sum_{\mathcal{S} \subseteq \mathcal{M}} (-1)^{k-|\mathcal{S}|}(q-1) \\ &= 1 - q + (q-1) \sum_{j=0}^{k} \binom{k}{j} (-1)^{k-j} \\ &= 1 - q.\end{aligned}$$

It is easily seen that these considerations imply the result. □

6. Estimating exponential sums occurring in the iteration process

In the present section we iterate the recurrence formula obtained in Section 5 for several times. This yields a new (more complicated) recurrence formula whose coefficients are exponential sums. Using the notions set up in Section 4 we give a nontrivial estimate for the coefficient of $X(I_1, \ldots, I_k, J; F_0, F_0)$. This is the key step in the proof of Theorem 3.3.

We now want to iterate Proposition 5.1. For this purpose we use the following abbreviations. $\mathcal{Q}_\ell := \{0, \ldots, q-1\}^\ell$. Furthermore, for vectors we use

$$\mathbf{r}_\ell = (r_{\ell 1}, \ldots, r_{\ell k}) \quad \text{and} \quad \mathbf{i}_\ell = (i_{\ell 1}, i_{\ell 2}).$$

Then the L-fold iteration of Proposition 5.1 yields

$$\begin{aligned}X(q^L I_1, \ldots, q^L I_k, q^L J; f_1, f_2) \;=\; & \sum_{\mathbf{r}_1, \ldots, \mathbf{r}_L \in \mathcal{Q}_k} \sum_{\mathbf{i}_1, \ldots, \mathbf{i}_L \in \mathcal{Q}_2} \\ & \left(\prod_{\ell=1}^{L} \alpha(\Xi_{\{\mathbf{r}_j, i_{j1}\}_{1 \le j \le \ell-1}}(f_1), \Xi_{\{\mathbf{r}_j, i_{j2}\}_{1 \le j \le \ell-1}}(f_2), \mathbf{r}_\ell, i_{\ell 1}, i_{\ell 2}) \right) \\ & \times X(I_1, \ldots, I_k, J; \Xi_{\{\mathbf{r}_\ell, i_{\ell 1}\}_{1 \le \ell \le L}}(f_1), \Xi_{\{\mathbf{r}_\ell, i_{\ell 2}\}_{1 \le \ell \le L}}(f_2)).\end{aligned} \tag{11}$$

Note that in the factor corresponding to $\ell = 1$ the set in the index of Ξ in the argument of α is empty. Thus the corresponding coefficient α reads $\alpha(f_1, f_2, \mathbf{r}_1, i_{11}, i_{12})$.

Now we select $L := L' + L'' + 3$ where L' and L'' are defined as in Section 4. Furthermore, let $k = d(q-1) + \rho$ with $0 \le \rho < q - 1$. We want to extract two summands from the sum in (11) which we will inspect more closely. The first summand is the one corresponding to the following selection.

$$\begin{array}{lll} \mathbf{r}_\ell = (0, \ldots, 0), & \mathbf{i}_\ell = (0,0) & (1 \le \ell \le L'), \\ \mathbf{r}_\ell = \mathbf{v}_1, & \mathbf{i}_\ell = \begin{cases} (1,1), & \text{if } \rho = 0 \\ (q-\rho, q-\rho), & \text{if } \rho > 0 \end{cases} & (\ell = L'+1), \\ \mathbf{r}_\ell = \mathbf{v}_{\ell - L'}, & \mathbf{i}_\ell = (0,0) & (L'+2 \le \ell \le L-3), \\ \mathbf{r}_\ell = (0, \ldots, 0), & \mathbf{i}_\ell = (q-1, 0) & (\ell = L-2), \\ \mathbf{r}_\ell = (0, \ldots, 0), & \mathbf{i}_\ell = (q-1, 0) & (\ell = L-1), \\ \mathbf{r}_\ell = (0, \ldots, 0), & \mathbf{i}_\ell = (0,0) & (\ell = L). \end{array}$$

We call the summand in (11) corresponding to this selection V_1. The second selection is the same as the first apart from

$$\mathbf{i}_{L-1} = (0,0) \quad \text{instead of} \quad \mathbf{i}_{L-1} = (q-1,0).$$

The summand in (11) corresponding to this selection will be called V_2. First we examine V_1. To this matter we use the abbreviation

$$A(f_1,f_2) \;:=\; \left(\prod_{\ell=1}^{L-2} \alpha(\Xi_{\{\mathbf{r}_j,i_{j1}\}_{1\le j\le \ell-1}}(f_1), \Xi_{\{\mathbf{r}_j,i_{j2}\}_{1\le j\le \ell-1}}(f_2), \mathbf{r}_\ell, i_{\ell 1}, i_{\ell 2})\right).$$

Note that from the definition of $\Xi_{\mathbf{r},i}$ we get

$$\begin{aligned} \Xi_{\mathbf{0},q-1}(F_0) &= F_0,\\ \Xi_{\mathbf{0},0}(F_1) &= F_0,\\ \Xi_{\mathbf{0},q-1}(F_1) &= F_1. \end{aligned} \tag{12}$$

Applying Lemma 4.2 we see that

$$\begin{aligned} \Xi_{\{\mathbf{r}_j,i_{j1}\}_{1\le j\le L-2}}(f_1) &= \Xi_{\{\mathbf{r}_j,i_{j1}\}_{L'+1\le j\le L-2}}(F_0)\\ &= \Xi_{\mathbf{0},q-1}(F_1)\\ &= F_1 \end{aligned} \tag{13}$$

(Lemma 4.2 (i) has been applied for the first, Lemma 4.2 (ii) for the second and (12) for the third equality). In an analogous way we see that

$$\Xi_{\{\mathbf{r}_j,i_{j2}\}_{1\le j\le L-2}}(f_2) = F_0. \tag{14}$$

All this yields together with (11) that

$$\begin{aligned} V_1 &= A(f_1,f_2)\\ &\quad \times\alpha(\Xi_{\{\mathbf{r}_j,i_{j1}\}_{1\le j\le L-2}}(f_1),\Xi_{\{\mathbf{r}_j,i_{j2}\}_{1\le j\le L-2}}(f_2),\mathbf{r}_{L-1},i_{L-1,1},i_{L-1,2})\\ &\quad \times\alpha(\Xi_{\{\mathbf{r}_j,i_{j1}\}_{1\le j\le L-1}}(f_1),\Xi_{\{\mathbf{r}_j,i_{j2}\}_{1\le j\le L-1}}(f_2),\mathbf{r}_L,i_{L1},i_{L2})\\ &\quad \times X(I_1,\dots,I_k,J;\Xi_{\{\mathbf{r}_j,i_{j1}\}_{1\le j\le L}}(f_1),\Xi_{\{\mathbf{r}_j,i_{j2}\}_{1\le j\le L}}(f_2))\\ &= A(f_1,f_2)\alpha(F_1,F_0,\mathbf{r}_{L-1},i_{L-1,1},i_{L-1,2})\\ &\quad \times\alpha(\Xi_{\mathbf{r}_{L-1},i_{L-1,1}}(F_1),\Xi_{\mathbf{r}_{L-1},i_{L-1,2}}(F_0),\mathbf{r}_L,i_{L1},i_{L2})\\ &\quad \times X(I_1,\dots,I_k,J;\Xi_{\{\mathbf{r}_j,i_{j1}\}_{L-1\le j\le L}}(F_1),\Xi_{\{\mathbf{r}_j,i_{j2}\}_{L-1\le j\le L}}(F_0))\\ &= A(f_1,f_2)\alpha(F_1,F_0,\mathbf{0},q-1,0)\alpha(F_1,F_0,\mathbf{0},0,0)\\ &\quad \times X(I_1,\dots,I_k,J;F_0,F_0). \end{aligned}$$

In the first equality we applied (13) and (14), the second equality follows from (12). In the same way we obtain

$$V_2 \;=\; A(f_1,f_2)\alpha(F_1,F_0,\mathbf{0},0,0)\alpha(F_0,F_0,\mathbf{0},0,0)X(I_1,\dots,I_k,J;F_0,F_0).$$

Now we can apply Lemma 5.1 in order to obtain

$$\begin{aligned} V_1 &= A(f_1,f_2)e\left(\frac{h}{m}(2-q)\right)X(I_1,\dots,I_k,J;F_0,F_0),\\ V_2 &= A(f_1,f_2)e\left(\frac{h}{m}\right)X(I_1,\dots,I_k,J;F_0,F_0). \end{aligned}$$

Thus we can rewrite (11) as

$$\begin{aligned} X(q^LI_1,\dots,q^LI_k,q^LJ;f_1,f_2) &= \\ \sum_D \left(\prod_{\ell=1}^{L} \alpha(\Xi_{\{\mathbf{r}_j,i_{j1}\}_{1\le j\le \ell-1}}(f_1),\Xi_{\{\mathbf{r}_j,i_{j2}\}_{1\le j\le \ell-1}}(f_2),\mathbf{r}_\ell,i_{\ell 1},i_{\ell 2})\right)& \\ \times X(I_1,\dots,I_k,J;\Xi_{\{\mathbf{r}_\ell,i_{\ell 1}\}_{1\le\ell\le L}}(f_1),\Xi_{\{\mathbf{r}_\ell,i_{\ell 2}\}_{1\le\ell\le L}}(f_2))+V_1+V_2.& \end{aligned}$$

Here D denotes the range of summation in (11) apart from the two selections of the parameters corresponding to V_1 and V_2.

If we rearrange the terms in this sum we arrive at

$$\begin{aligned} X(q^LI_1,\dots,q^LI_k,q^LJ;f_1,f_2) = &\\ &\left(\sum_{\substack{g_1,g_2\in\mathcal{F}\\ (g_1,g_2)\ne(F_0,F_0)}} a'(f_1,f_2,g_1,g_2)X(I_1,\dots,I_k,J;g_1,g_2)\right)\\ &+\left(a'(F_0,F_0)+A(f_1,f_2)\left(e\left(\frac{h}{m}(2-q)\right)+e\left(\frac{h}{m}\right)\right)\right)\\ &\times X(I_1,\dots,I_k,J;F_0,F_0), \end{aligned}$$

where $a'(g_1,g_2)$ is the sum of all $\alpha(\cdot)$, which occur as coefficients of $X(g_1,g_2)$ in the sum over D. Since D has $q^{k+2}L-2$ summands each of which has a coefficient of modulus 1, we conclude that for all $f_1,f_2\in\mathcal{F}$

$$\sum_{g_1,g_2\in F}|a'(f_1,f_2,g_1,g_2)|\le q^{(k+2)L}-2.$$

Set

$$\begin{aligned} a(f_1,f_2,g_1,g_2) &:= a'(f_1,f_2,g_1,g_2) \quad \text{if} \quad (g_1,g_2)\ne(F_0,F_0),\\ a(f_1,f_2,F_0,F_0) &:= a'(f_1,f_2,F_0,F_0)+A(f_1,f_2)\left(e\left(\frac{h}{m}(2-q)\right)+e\left(\frac{h}{m}\right)\right). \end{aligned}$$

Since $m\nmid h(q-1)$ we have

$$\left|e\left(\frac{h}{m}(2-q)\right)+e\left(\frac{h}{m}\right)\right|\le\left|1+e\left(\frac{1}{m}\right)\right|\le 2-\left(\frac{\pi}{2m}\right)^2.$$

Thus

$$\sum_{g_1,g_2\in F} |a(f_1,f_2,g_1,g_2)| \leq q^{(k+2)L} - \left(\frac{\pi}{2m}\right)^2. \tag{15}$$

Let B be the $|\mathcal{F}|^2 \times |\mathcal{F}|^2$ matrix

$$B := (|a(f_1,f_2,g_1,g_2)|)_{(f_1,f_2)\in\mathcal{F}^2,(g_1,g_2)\in\mathcal{F}^2}. \tag{16}$$

Then we conclude that

$$(|X(q^LI_1,\ldots,q^LI_k,q^LJ;f_1,f_2)|)_{(f_1,f_2)\in\mathcal{F}^2} \leq B\,(|X(I_1,\ldots,I_k,J;g_1,g_2)|)_{(g_1,g_2)\in\mathcal{F}^2}. \tag{17}$$

The inequality is meant componentwise.

7. Proof of the correlation result

In this section we finish the proof of Theorem 3.3. The remaining part of this proof proceeds along similar lines as Kim [15, p. 325–328].

First define the abbreviations

$$p := q^L \qquad \text{and} \qquad \varepsilon := \frac{\pi^2}{4m^2p^{k+2}}.$$

By (15) the row sums of the matrix B in (16) are less than or equal to $p^{k+2}(1-\varepsilon)$. Since all the entries of B are non-negative, this implies that for each $\ell\in\mathbb{N}$ the row sums in B^ℓ are less than or equal to $p^{(k+2)\ell}(1-\varepsilon)^\ell$. Thus the ℓ-fold iteration of the matrix inequality (17) together with the trivial estimate

$$|X(I_1,\ldots,I_k,J;f_1,f_2)| \leq |I_1|\cdots|I_k||J|^2$$

yields

$$|X(p^\ell I_1,\ldots,p^\ell I_k,p^\ell J;f_1,f_2)| \leq (1-\varepsilon)^\ell (p^\ell|I_1|)\cdots(p^\ell|I_k|)(p^\ell|J|)^2. \tag{18}$$

Set

$$t := \left\lfloor \frac{10\log N}{21\log p} \right\rfloor;$$

then $p^t < \sqrt{N}$. Now let

$$I_j = [a_j,b_j] \quad (1\leq j\leq k), \qquad J=[a_{k+1},b_{k+1}]$$

be the intervals occurring in the statement of Theorem 3.3. Then we can write

$$a_j = p^tu_j + r_j \qquad \text{and} \qquad b_j = p^tv_j+s_j \qquad (1\leq j\leq k+1)$$

with $0\leq r_j,s_j<p^t$ in a unique way. Here $|u_j-v_j|\geq 1$ because all the intervals have length greater than $\sqrt{N}$ by assumption. Now set

$$\tilde{I}_j := [u_j,v_j] \quad (1\leq j\leq k), \qquad \tilde{J} := [u_{k+1},v_{k+1}].$$

From the definition of X (note that the summands in the innermost sum have all modulus 1) we easily derive

$$X(I_1,\ldots,I_k,J;f_1,f_2) = X(p^t\tilde{I}_1,\ldots,p^t\tilde{I}_k,p^t\tilde{J};f_1,f_2) + \mathcal{O}\left(|I_1|\cdots|I_k||J|^2\frac{p^t}{\sqrt{N}}\right). \tag{19}$$

Since $(1-\varepsilon)^t < e^{-t\varepsilon}$, (19) yields together with (18) the estimate

$$X(I_1,\ldots,I_k,J;f_1,f_2) \ll \left(e^{-t\varepsilon}+\frac{p^t}{\sqrt{N}}\right)|I_1|\cdots|I_k||J|^2. \tag{20}$$

From the definition of t we easily derive (if N is large enough)

$$-\varepsilon t \le -\frac{10\log N}{22\log p}\frac{\pi^2}{4m^2p^{k+2}} \le -\frac{\log N}{m^2p^{k+2}\log p} \le -\frac{\log N}{m^2q^{L(k+2)+1}}.$$

Since $L=L'+L''<2\frac{k}{q-1}+2$ this yields

$$-\varepsilon t \le -\frac{\log N}{m^2q^{p(q,k)}}$$

with $p(q,k)$ as in (3). Furthermore,

$$\frac{p^t}{\sqrt{N}} \le \frac{\exp\left(\frac{10}{21}\log N\right)}{\sqrt{N}} = N^{-\frac{1}{42}}.$$

Inserting this in (20) and specializing $f_1=f_2=F_0$ yields Theorem 3.3.

8. Proof of the "digital" version of Weyl's Lemma

In this section we want to show Theorem 3.4. The proof will be done by using the first part of ordinary Weyl's Lemma (cf. [25, Lemma 2.3]) together with the correlation result in Theorem 3.3. Let φ be an arithmetic function. The sum in Theorem 3.4 is of the shape

$$T(\varphi) := \sum_{n<N} e(\varphi(n)). \tag{21}$$

The following lemma is the starting point for the deduction of the estimate in Theorem 3.4.

Lemma 8.1 (first part of Weyl's Lemma, cf. [25, Lemma 2.3])**.** *Let $T(\varphi)$ be as in* (21). *Then the estimate*

$$|T(\varphi)|^{2^j} \le (2N)^{2^j-j-1}\sum_{|h_1|<N}\cdots\sum_{|h_j|<N} T_j$$

holds. Here

$$T_j := \sum_{n\in H_j(h_1,\ldots,h_j)} e(\Delta_j(\varphi(n);h_1,\ldots,h_j))$$

and the integer intervals H_ℓ satisfy

$$\begin{aligned} H_1(h_1) &\subseteq [1,N]\cap\mathbb{N}, \\ H_\ell(h_1,\ldots,h_\ell) &= H_{\ell-1}(h_1,\ldots,h_{\ell-1}) \cap \{x \mid x+h_\ell \in H_{\ell-1}(h_1,\ldots,h_{\ell-1})\}. \end{aligned}$$

In what follows, we need the k-th differences

$$\Delta_k\left(\theta n^k+\frac{\ell}{m}s_q(n);h_1,\dots,h_k\right). \tag{22}$$

It is easy to see that the difference operators Δ_j are linear. Thus we may treat the summands in (22) separately. It is well known that

$$\Delta_k(\theta n^k;h_1,\dots,h_k)=\theta k!h_1\cdots h_k.$$

Furthermore, linearity of Δ_k yields

$$\Delta_k\left(\frac{\ell}{m}s_q(n);h_1,\dots,h_k\right)=\frac{\ell}{m}\Delta_k\left(s_q(n);h_1,\dots,h_k\right).$$

Using these two identities and applying Lemma 8.1 with $\varphi(n)=\theta n^k+\frac{\ell}{m}s_q(n)$ we arrive at

$$\begin{aligned}\left|T\left(\theta n^k+\frac{\ell}{m}s_q(n)\right)\right|^{2^k} \leq\; & \\ &\left|(2N)^{2^k-k-1}\sum_{|h_1|<N}\cdots\sum_{|h_k|<N}\sum_{n\in H_k(h_1,\dots,h_k)}\right.\\ &\left. e\left(\theta h_1\cdots h_k k!+\frac{\ell}{m}\Delta_k(s_q(n);h_1,\dots,h_k)\right)\right|\\ =&\left|(2N)^{2^k-k-1}\sum_{|h_1|<N}\cdots\sum_{|h_k|<N}\right.\\ &\left. e\left(\theta h_1\cdots h_k k!\right)\sum_{n\in H_k(h_1,\dots,h_k)}e\left(\frac{\ell}{m}\Delta_k(s_q(n);h_1,\dots,h_k)\right)\right|.\end{aligned}$$

Shifting the modulus to the innermost sum yields

$$\begin{aligned}\left|T\left(\theta n^k+\frac{\ell}{m}s_q(n)\right)\right|^{2^k} \leq\;& (2N)^{2^k-k-1}\sum_{|h_1|<N}\cdots\sum_{|h_k|<N}\\ &\left|\sum_{n\in H_k(h_1,\dots,h_k)}e\left(\frac{\ell}{m}\Delta_k(s_q(n);h_1,\dots,h_k)\right)\right|.\end{aligned} \tag{23}$$

The sum in (23) resembles the sum estimated in Theorem 3.3. The only defects are the following.

- The range of the innermost sum depends on $h_1,\dots,h_k$.
- The modulus of the innermost sum is not squared.

The first of these defects can be mended by splitting the sums in several blocks of reasonable size. In these blocks the range of the innermost sum can be made constant at the cost of an error term which is small enough to be harmless. The second defect can be easily removed by an application of the Cauchy-Schwarz inequality.

Let η be as in Theorem 3.3 and select real numbers $\alpha, \beta, \varepsilon$ with

$$\alpha > \frac{\eta}{2}, \quad \beta \geq \frac{1}{2}, \quad \alpha + \beta = 1, \quad 0 < \varepsilon \leq \alpha - \frac{\eta}{2}.$$

With these selections we can rewrite the sum

$$S := \sum_{|h_1|<N} \cdots \sum_{|h_k|<N} \left| \sum_{n \in H_k(h_1,\ldots,h_k)} e\left(\frac{\ell}{m}\Delta_k(s_q(n); h_1, \ldots, h_k)\right) \right|$$

by decomposing the sums outside the modulus in blocks of length $\lfloor N^\beta \rfloor$ as follows.

$$S = \sum_{j_1=-\lfloor N^\alpha \rfloor -1}^{\lfloor N^\alpha \rfloor +1} \cdots \sum_{j_k=-\lfloor N^\alpha \rfloor -1}^{\lfloor N^\alpha \rfloor +1} R(j_1, \ldots, j_k) + \mathcal{O}\left(N^{k\beta+1}\right) \tag{24}$$

with

$$R(j_1, \ldots, j_k) := \sum_{h_1=j_1\lfloor N^\beta \rfloor}^{(j_1+1)\lfloor N^\beta \rfloor -1} \cdots \sum_{h_k=j_k\lfloor N^\beta \rfloor}^{(j_k+1)\lfloor N^\beta \rfloor -1} \left| \sum_{n \in H_k(h_1,\ldots,h_k)} e\left(\frac{\ell}{m}\Delta_k(s_q(n); h_1, \ldots, h_k)\right) \right|.$$

Now we want to estimate the sums $R(j_1, \ldots, j_k)$. To this matter we distinguish two cases.

(i) Suppose that $|H_k(h_1, \ldots, h_k)| > N^{\beta+\varepsilon}$ for all

$$j_r\lfloor N^\beta \rfloor \leq h_r < (j_r+1)\lfloor N^\beta \rfloor \qquad (1 \leq r \leq k). \tag{25}$$

From Lemma 8.1 one can easily see that the bounds of the interval $H(h_1, \ldots, h_k)$ depend linearly on $h_1, \ldots, h_k$. Furthermore, by (25) each of these variables can vary only in an interval of length $\lfloor N^\beta \rfloor$. Thus there exist positive integers u and v such that

$$H(h_1, \ldots, h_k) = \left[u + \mathcal{O}\left(N^\beta\right), v + \mathcal{O}\left(N^\beta\right)\right] \cap \mathbb{N}$$

for each k-tuple $(h_1, \ldots, h_k)$ satisfying (25). The implied constants are easily seen to be uniform in $j_1, \ldots, j_k$. Now set

$$H'(j_1, \ldots, j_k) := [u, v] \cap \mathbb{N}.$$

$H'(j_1, \ldots, j_k)$ is independent of $(h_1, \ldots, h_k)$ as long as (25) holds. Furthermore, it satisfies

$$|H'(j_1, \ldots, j_k) \bigtriangleup H(h_1, \ldots, h_k)| \ll N^\beta$$

where $\triangle$ denotes the symmetric difference. Thus we get

$$\begin{aligned} R(j_1,\dots,j_k) &= \sum_{h_1=j_1\lfloor N^\beta\rfloor}^{(j_1+1)\lfloor N^\beta\rfloor-1}\cdots\sum_{h_k=j_k\lfloor N^\beta\rfloor}^{(j_k+1)\lfloor N^\beta\rfloor-1} \\ &\quad \left|\sum_{n\in H_k'(j_1,\dots,j_k)} e\left(\frac{\ell}{m}\Delta_k(s_q(n);h_1,\dots,h_k)\right)\right| \\ &\quad +\mathcal{O}\left(N^{(k+1)\beta}\right). \end{aligned}$$

Applying the Cauchy-Schwarz inequality yields

$$\begin{aligned} R(j_1,\dots,j_k) &= \left(N^{k\beta}\sum_{h_1=j_1\lfloor N^\beta\rfloor}^{(j_1+1)\lfloor N^\beta\rfloor-1}\cdots\sum_{h_k=j_k\lfloor N^\beta\rfloor}^{(j_k+1)\lfloor N^\beta\rfloor-1}\right. \\ &\quad \left.\left|\sum_{n\in H_k'(j_1,\dots,j_k)} e\left(\frac{\ell}{m}\Delta_k(s_q(n);h_1,\dots,h_k)\right)\right|^2\right)^{\frac{1}{2}} \\ &\quad +\mathcal{O}\left(N^{(k+1)\beta}\right). \end{aligned}$$

Since $\beta\geq\frac{1}{2}$ the conditions for the applications of Theorem 3.3 are satisfied and an application of this theorem yields

$$R(j_1,\dots,j_k)\ll N^{k\beta+1-\frac{\eta}{2}}+N^{(k+1)\beta}\ll N^{k\beta+1-\frac{\eta}{2}}. \tag{26}$$

(ii) Now suppose at the contrary that $|H_k(h_1,\dots,h_k)|\leq N^{\beta+\varepsilon}$ for at least one k-tuple $(h_1,\dots,h_k)$ satisfying (25). Since the bounds of the interval $H(h_1,\dots,h_k)$ depend linearly on $h_1,\dots,h_k$, this implies that

$$|H_k(h_1,\dots,h_k)|\ll N^{\beta+\varepsilon}$$

holds for all k-tuples $(h_1,\dots,h_k)$. Thus estimating $R(j_1,\dots,j_k)$ trivially in this case yields

$$R(j_1,\dots,j_k)\ll N^{(k+1)\beta+\varepsilon}\ll N^{k\beta+1-\frac{\eta}{2}}. \tag{27}$$

Inserting (26) and (27) in (24) we arrive at

$$S\ll N^{k\alpha+k\beta+1-\frac{\eta}{2}}=N^{k+1-\frac{\eta}{2}}.$$

Using this in (23) we get

$$\left|T\left(\theta n^k+\frac{\ell}{m}s_q(n)\right)\right|^{2^k}\ll N^{2^k-\frac{\eta}{2}}.$$

Taking the 2^k-th root yields the result.

9. Application of the circle method

In this section we will prove Theorem 3.2. Then we will indicate how this proof has to be modified in order to get Theorem 3.1. We do it this way in order to avoid cumbersome notations in the proof. First we want to reformulate the problem of expressing integers in the way indicated in Theorem 3.2 in terms of exponential sums. To this matter we will use the well-known circle method (cf. for instance Vaughan [25]).

Let

$$P := \lfloor N^{1/k} \rfloor$$

and let $F(z)$ be given by the series

$$F(z) := \sum_{n \in U_{h,m}(P)} z^{n^k}.$$

Then $F(z)^s$ can be expanded in a Taylor series

$$F(z)^s = \sum_{n \geq 0} C_n z^n.$$

It is easy to see that C_N is the number of representations of N as

$$N = x_1^k + \cdots + x_s^k, \qquad x_j \in U_{h,m}(P).$$

Thus in order to show Theorem 3.2 we need the asymptotic behaviour of the coefficients C_N of this Taylor series. Cauchy's formula yields that

$$\begin{aligned} C_N &= \frac{1}{2\pi i} \oint F(z)^s z^{-N-1} dz \\ &= \int_0^1 \sum_{n_1 \in U_{h,m}(P)} \cdots \sum_{n_s \in U_{h,m}(P)} e\left(\theta(n_1^k + \cdots + n_s^k - N)\right) d\theta. \end{aligned}$$

In order to get rid of the set $U_{h,m}(P)$ in the range of summation we use a trick which goes back to Gelfond [12]. Namely, for an arithmetic function φ set

$$H_\ell(\varphi, P) := \sum_{n=0}^{P-1} e\left(\varphi(n) + \frac{\ell}{m} s_q(n)\right).$$

Then

$$\begin{aligned} \sum_{\ell=0}^{m-1} e\left(-\frac{\ell h}{m}\right) H_\ell(\varphi, P) &= \sum_{n=0}^{P-1} \sum_{\ell=0}^{m-1} e\left(\ell \frac{s_q(n) - h}{m}\right) e(\varphi(n)) \\ &= m \sum_{n \in U_{h,m}(P)} e(\varphi(m)). \end{aligned}$$

With help of this identity we may write

$$\begin{aligned}\sum_{n\in U_{h,m}(P)} e\left(\theta n^k\right) &= \sum_{\ell=0}^{m-1} e\left(-\frac{\ell h}{m}\right) H_\ell(\theta n^k, P)\\ &= \frac{1}{m}\sum_{\ell=0}^{m-1}\sum_{n=0}^{P-1} e\left(\ell\frac{s_q(n)-h}{m}\right) e(\theta n^k).\end{aligned}$$

Inserting this in the integral representation of C_N we arrive at

$$\begin{aligned}C_N &= \frac{1}{m^s}\int_0^1 \sum_{n_1<P}\cdots\sum_{n_s<P}\sum_{\ell_1=0}^{m-1}\cdots\sum_{\ell_s=0}^{m-1}\\ &\qquad e\left(\ell_1\frac{s_q(n_1)-h}{m}\right)\cdots e\left(\ell_s\frac{s_q(n_s)-h}{m}\right) e\left(\theta(n_1^k+\ldots+n_s^k-N)\right) d\theta.\end{aligned}$$

The integral can be split in two parts, one corresponding to the selection $\ell_1=\cdots=\ell_s=0$, the other corresponding to the remaining selections for the ℓ_j. We get

$$\begin{aligned}C_N &= \frac{1}{m^s}\int_0^1 \sum_{n_1<P}\cdots\sum_{n_s<P} e\left(\theta\left(n_1^k+\cdots+n_s^k-N\right)\right) d\theta\\ &\quad+\frac{1}{m^s}\int_0^1 \sum_{n_1<P}\cdots\sum_{n_s<P}\underbrace{\sum_{\ell_1=0}^{m-1}\cdots\sum_{\ell_s=0}^{m-1}}_{\ell_1+\cdots+\ell_s\neq 0}\\ &\qquad e\left(\ell_1\frac{s_q(n_1)-h}{m}\right)\cdots e\left(\ell_s\frac{s_q(n_s)-h}{m}\right) e\left(\theta(n_1^k+\cdots+n_s^k-N)\right) d\theta\\ &=: \mathcal{I}_1+\mathcal{I}_2.\end{aligned}$$

The integral $\mathcal{I}_1$ is well-known from the ordinary Waring's problem and can be treated along the known lines. This integral will contribute the main term in Theoren 3.2. Thus we are left with the integral $\mathcal{I}_2$. Let $L=(\ell_1,\ldots,\ell_s)\neq 0$. Then $\mathcal{I}_2$ consists of integrals of the shape

$$\begin{aligned}\mathcal{J}_L &:= \int_0^1 \left(\sum_{n_1<P} e\left(\theta n_1^k+\ell_1\frac{s_q(n_1)-h}{m}\right)\right)\cdots\\ &\qquad\left(\sum_{n_s<P} e\left(\theta n_s^k+\ell_s\frac{s_q(n_s)-h}{m}\right)\right) e(-N\theta)d\theta.\end{aligned}$$

It turns out that these integrals do not contribute to the main term, i.e. we have no major arcs.

For convenience set

$$S_j(\theta) := \sum_{n<P} e\left(\theta n^k+\frac{\ell_j}{m}s_q(n)\right).$$

Since $s > 2^k$ we can estimate $\mathcal{J}_L$ by

$$|\mathcal{J}_L| \le \sup_{\theta,j} \left(|S_j(\theta)|^{s-2^k}\right) \max_t \left(\int_0^1 |S_t(\theta)|^{2^k} d\theta\right). \tag{28}$$

Analgously to the proof of the classical Lemma of Hua (cf. [25, Lemma 2.5]) we rewrite the last integral as

$$\int_0^1 |S_t(\theta)|^{2^k} d\theta \quad = \quad \sum_{n_1,\ldots,n_{2^k}} e\left(\ell_t \sum_{r=1}^{2^{k-1}} s_q(n_r) - s_q(n_{2^{k-1}+r})\right). \tag{29}$$

Here the sum is extended over all $n_1, \ldots, n_{2^k} < P$ fulfilling

$$n_1^k + \cdots + n_{2^{k-1}}^k = n_{2^{k-1}+1}^k + \cdots + n_{2^k}^k.$$

Thus the sum in (29) can be obviously estimated by

$$\left|\left\{n_1, \ldots, n_{2^k} < P \,\middle|\, n_1^k + \ldots + n_s^k = n_{s+1}^k + \ldots + n_{2s}^k\right\}\right|.$$

Applying Vaughan [24, Theorem 2] this yields

$$\int_0^1 |S_t(\theta)|^{2^k} d\theta \ll P^{2^k - k}.$$

Inserting this together with Theorem 3.4 in estimate (28) we arrive at

$$\mathcal{J}_L \ll P^{s-k-\gamma}.$$

The last estimate follows from the lower bound for s.

Summing up we have shown that $\mathcal{J}_L \ll P^{s-k-\gamma}$ for all $L \neq (0, \ldots, 0)$. This implies that

$$\mathcal{I}_2 \ll P^{s-k-\gamma}.$$

As mentioned above, the integral $\mathcal{I}_1$ is m^{-s} times the integral occurring in the ordinary Waring's problem. Thus its evaluation yields m^{-s} times the known Hardy-Littlewood asymptotic formula (cf. for instance Vaughan [25, Theorem 2.6]). Adding $\mathcal{I}_1$ and $\mathcal{I}_2$ yields Theorem 3.2. Note that only $\mathcal{I}_1$ contributes to the main term.

In order to prove Theorem 3.1 we start with the functions

$$F_i(z) := \sum_{\substack{n<P \\ s_{q_i}(n) \equiv h_i(m_i)}} z^{n^k} \qquad (1 \le j \le s).$$

In what follows we have to work with

$$\prod_{i=1}^s F_i(z)$$

instead of $F(z)^s$. This does not alter the proof. The only difference is that we have to keep track of the indices of h_i, m_i and q_i.

10. Concluding remarks

We already mentioned in Remark 3.2 that there is some space to improve the bound for s in Theorem 3.2. We even think that the following should be true.

Conjecture 10.1. *For each $k \in \mathbb{N}$*

$$G_{h,m}(k) = G(k)$$

holds for all $h, m \in \mathbb{N}$.

By Wooley [31] this would imply a big improvement for the bound of s in our result. For the case $k = 2$ the conjecture would yield that Lagrange's theorem on the representability of integers as sum of four squares holds asymptotically with digital restrictions. Of course, one can not expect a similar result for $g_{h,m}(k)$, whose value depends at least on m.

In this context it would be interesting to determine $g_{h,m}(k)$ at least for special values of h, m and k. Even for $k = 1$ this seems to be a nontrivial problem.

References

[1] A. Balog and A. Sárközy. On sums of integers having small prime factors I. *Studia Sci. Math. Hungar.*, 19:35–47, 1984.

[2] R. Bellman and H. N. Shapiro. On a problem in additive number theory. *Ann. of Math. (2)*, 49:333–340, 1948.

[3] J. Bésineau. Indépendance statistique d'ensembles liés à la fonction "somme des chiffres". *Acta Arith.*, 20:401–416, 1972.

[4] J. Brüdern. A sieve approach to the Waring-Goldbach problem. I. Sums of four cubes. *Ann. Sci. École Norm. Sup. (4)*, 28:461–476, 1995.

[5] J. Brüdern. A sieve approach to the Waring-Goldbach problem. II. On the seven cubes theorem. *Acta Arith.*, 72:211–227, 1995.

[6] J. Brüdern and E. Fouvry. Lagrange's four squares theorem with almost prime variables. *J. Reine Angew. Math.*, 454:59–96, 1994.

[7] H. Delange. Sur la fonction sommatoire de la fonction "somme des chiffres". *Enseign. Math. (2)*, 21:31–47, 1975.

[8] M. Drmota and J. Schoissengeier. Digital expansions with respect to different bases. *Monatsh. Math.*, to appear.

[9] K. B. Ford. New estimates for mean values of Weyl sums. *Internat. Math. Res. Notices*, (3):155–171 (electronic), 1995.

[10] E. Fouvry and C. Mauduit. Méthodes de crible et fonctions sommes des chiffres. *Acta Arith.*, 77:339–351, 1996.

[11] E. Fouvry and C. Mauduit. Sommes des chiffres et nombres presque premiers. *Math. Ann.*, 305(3):571–599, 1996.

[12] A. O. Gelfond. Sur les nombres qui ont des propriétés additives et multiplicatives données. *Acta Arith.*, 13:259–265, 1968.

[13] G. Harcos. Waring's problem with small prime factors. *Acta Arith.*, 80:165–185, 1997.

[14] L.-K. Hua. *Additive theory of prime numbers.* Translations of Mathematical Monographs, Vol. 13 American Mathematical Society, Providence, R.I. 1965

[15] D.-H. Kim. On the joint distribution of q-additive functions in residue classes. *J. Number Theory*, 74:307–336, 1999.

[16] C. Mauduit and A. Sárközy. On the arithmetic structure of sets characterized by sum of digits properties. *J. Number Theory*, 61:25–38, 1996.

[17] C. Mauduit and A. Sárközy. On the arithmetic structure of integers, whose sum of digits functionis fixed. *Acta Arith.*, 81:145–173, 1997.
[18] M. B. Nathanson. *Additive number theory. The classical bases.*, volume 164 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.
[19] M. B. Nathanson. *Additive number theory. Inverse problems and the geometry of sumsets.*, volume 165 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.
[20] A. Pethő and R. F. Tichy. S-unit equations, linear recurrences and digit expansions. *Publ. Math. Debrecen*, 42(1-2):145–154, 1993.
[21] H. P. Schlickewei. Linear equations in integers with bounded sum of digits. *J. Number Theory*, 35(3):335–344, 1990.
[22] C. L. Stewart. On the representation of an integer in two different bases. *J. Reine Angew. Math.*, 319:63–72, 1980.
[23] J. M. Thuswaldner and R. F. Tichy. An Erdős-Kac theorem for systems of q-additive functions. *Indag. Math. (N.S.)*, 11(2):283–291, 2000.
[24] R. C. Vaughan. On Waring's problem for smaller exponents. II. *Mathematika* 33:6–22, 1986.
[25] R. C. Vaughan. *The Hardy-Littlewood method*, volume 125 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, second edition, 1997.
[26] R. C. Vaughan and T. D. Wooley. Further improvements in Waring's problem. *Acta Math.* 174:147–240, 1995.
[27] R. C. Vaughan and T. D. Wooley. Further improvements in Waring's problem. II. Sixth powers. *Duke Math. J.* 76:683–710, 1994.
[28] R. C. Vaughan and T. D. Wooley. Further improvements in Waring's problem. III. Eighth powers. *Philos. Trans. Roy. Soc. London Ser. A* 345:385–396, 1993.
[29] R. C. Vaughan and T. D. Wooley. Further improvements in Waring's problem. IV. Higher powers. *Acta Arith.* 94:203–285, 2000.
[30] I. M. Vinogradov. *The method of trigonometrical sums in the theory of numbers.* Translated, revised and annotated by K. F. Roth and Anne Davenport. Interscience Publishers, London and New York. no year given.
[31] T. D. Wooley. Large improvements in Waring's problem. *Ann. of Math. (2)*, 135(1):131–164, 1992.

Institut für Mathematik und Angewandte Geometrie, Abteilung für Mathematik und Statistik, Montanuniversität Leoben, Franz-Josef-Strasse 18, A-8700 Leoben, AUSTRIA
E-mail address: `joerg.thuswaldner@unileoben.ac.at`

Institut für Mathematik 501 (A), Technische Universität Graz, Steyrergasse 30, A-8020 Graz, AUSTRIA
E-mail address: `tichy@tugraz.at`