

A HYBRID RESULT RELATED TO WARING'S PROBLEM, SQUAREFREE NUMBERS, AND DIGITAL RESTRICTIONS

Martin **Jancevskis**

Technische Universität Graz, Institut für Mathematik A, Steyrergasse 30, 8010 Graz, Austria

Received: November 2009

MSC 2000: 11 P 05, 11 A 63

Keywords: Waring's Problem, digital restrictions, squarefree numbers.

Abstract: Let $s > 2^k$ and let $s_q(\cdot)$ denote the sum-of-digits-function to an integer base q . Under certain mild conditions, we prove that

$$N = x_1^k + \dots + x_s^k$$

has a solution for almost all integers N where for all $i = 1, \dots, s$, the variables x_i are assumed to be squarefree and fulfill the additive condition $s_{q_i}(n) \equiv h_i \pmod{m_i}$ for given integers q_i .

1. Introduction

Let $q \geq 2$. A positive integer n admits the unique representation

$$n = \sum_{j \geq 0} a_j q^j$$

in the q -adic numeration system, where $0 \leq a_j < q$ for all $j \in \mathbb{N}$. Let

$$s_q(n) := \sum_{j \geq 0} a_j$$

E-mail address: jancevskis@tugraz.at

The author was supported by the Austrian Science Foundation (FWF), projects S9610 and S9611, and wants to thank J. Thuswaldner and R. Tichy for helpful discussions.

be the sum-of-digits function. Its basic property – called q -additivity – is that $s_q(nq^h + m) = s_q(n) + s_q(m)$ holds for all $n, m, h \in \mathbb{N}$ with $m < q^h$. The sum-of-digits function has been extensively studied since the publication of a paper of Gelfond [4] in 1967. Let μ denote the Möbius μ -function, that is $\mu(n) = 0$ if n is not a squarefree integer, $\mu(n) = 1$ if n is a squarefree positive integer with an even number of distinct prime factors, and $\mu(n) = -1$ elsewhere.

For instance, for integers h, m with $m > 1$, Gelfond [4, Th. 2] showed that the condition that n is squarefree, i.e.

$$(1) \quad \mu^2(n) = 1,$$

and the condition

$$(2) \quad s_q(n) \equiv h \pmod{m}$$

are in a certain sense independent, i.e. the density of integers n such that (1) and (2) holds is

$$\frac{1}{m} \frac{6}{\pi^2},$$

as one expects, since we recall that the density of squarefree numbers is $6/\pi^2$. Recently, Mauduit and Rivat [7] proved that there are infinitely many primes p such that (2) holds with p in place of n . In particular, the number of primes smaller X that respect the additive condition (2) equals asymptotically $1/m$ times the number of all primes smaller X , as one might conjecture.

On a philosophical view, such results show that certain properties among the integers are independent. In this paper, we want to generalize this approach and study the independence of the conditions (1) and (2) among the set of solutions $(x_1, \dots, x_s) \in \mathbb{N}^s$ of

$$(3) \quad N = x_1^k + \dots + x_s^k,$$

where $s, k \in \mathbb{N}$ and N is a given positive integer. If one does not assume any restrictions to the variables x_j ($j = 1, \dots, s$) in (3), then the solvability of this equation is known as Waring's Problem.

Let $R_{k,s}(N)$ denote the number of solutions of (3) without restrictions on the variables. Let $s > 2^k$. It is well known that one has

$$R_{k,s}(N) \sim \mathfrak{S}_{k,s}(N) N^{s/k-1},$$

where $0 < \mathfrak{S}_{k,s}(N) \ll 1$ is an arithmetical function. We refer the reader to [10] for a survey. Before stating our main theorem, we introduce results on Waring's Problem where the variables are assumed to fulfill on the one hand (1) or on the other hand (2).

1.1. Waring's Problem with squarefree variables and generalizations

Among others, Waring's Problem with squarefree variables has been studied by Estermann [3] and by Baker and Brüdern [1], [2].

In the case $k = 2$, $s \geq 5$, Estermann [3, Formula 48] proved that the number of solutions of

$$(4) \quad N = x_1^2 + \dots + x_s^2$$

with $\mu^2(x_1) = \dots = \mu^2(x_s) = 1$ equals asymptotically

$$\mathfrak{S}_{2,s,\mu^2}(N)N^{s/2-1},$$

where \mathfrak{S}_{2,s,μ^2} is some arithmetical function. Thus $\mathfrak{S}_{2,s,\mu^2}(N) > 0$ implies that (4) has a solution with x_j squarefree ($j = 1, \dots, s$) for sufficiently large N . According to [3, Th. 1], $\mathfrak{S}_{2,s,\mu^2}(N) \gg 1$ is fulfilled if the following Condition A holds.

A: Let (N, s) be said to satisfy Condition A if

$$x_1^2 + \dots + x_s^2 \equiv N \pmod{32}$$

has a solution with $4 \nmid x_j$ for $j = 1, \dots, s$.

Condition A holds for all N if $s \geq 8$.

In a previous paper [6], we proved an asymptotic formula for the number $R_{k,s,\mu^2}(N)$ of solutions of (3) where the variables x_j ($j = 1, \dots, s$) are assumed to be squarefree. For $s > 2^k$, we showed that there is some $\rho > 0$ such that

$$(5) \quad R_{k,s,\mu^2}(N) = \mathfrak{S}_{k,s,\mu^2}(N)N^{s/k-1} + O(N^{s/k-1-\rho})$$

holds. One has $\mathfrak{S}_{k,s,\mu^2}(N) > 0$ if $k \geq 3$ or Condition A holds.

Now we want to generalize the notion of squarefree integers. Let \mathcal{V} be a set of pairwise coprime integers not containing 1. Throughout this paper, we assume that there is some $\delta > 0$ such that

$$(6) \quad \sum_{v \in \mathcal{V}} \frac{1}{v^{1-\delta}}$$

converges. Introduce

$$\chi_{\mathcal{V}}(n) := \begin{cases} 1 & \text{if } v \nmid n \text{ for all } v \in \mathcal{V}; \\ 0 & \text{otherwise.} \end{cases}$$

We are interested in the set $\{n \in \mathbb{N} : \chi_{\mathcal{V}}(n) = 1\}$. One of the most prominent examples is the set of squarefree numbers. In this case $\mathcal{V} = \{p^2 : p \text{ prime}\}$ and we have $\chi_{\mathcal{V}} = \mu^2$. Now, for any $\varepsilon > 0$ and $\delta = 1/2 - \varepsilon$ our assumption (6) holds. We refer the reader to [5] for details to these sieve sequences.

Let $s, k \in \mathbb{N}$. We denote by $R_{k,s,\mathcal{V}}(N)$ the number of solutions of (3) with $\chi_{\mathcal{V}}(x_1) = \dots = \chi_{\mathcal{V}}(x_s) = 1$.

In [6] we showed that there is some $\rho > 0$ such that

$$(7) \quad R_{k,s,\mathcal{V}}(N) = \mathfrak{S}_{k,s,\mathcal{V}}(N) N^{s/k-1} + O(N^{s/k-1-\rho}),$$

for some arithmetic function $\mathfrak{S}_{k,s,\mathcal{V}}(N) \ll 1$. Unfortunately, we could not determine whether $\mathfrak{S}_{k,s,\mathcal{V}}(N) > 0$ for an arbitrary set \mathcal{V} of pairwise coprime integers. Indeed, $\mathfrak{S}_{\mathcal{V}}(N) \ll 1$ can not hold in general. For instance, if $2 \in \mathcal{V}$, then all variables x_i are odd. And N has to be even (odd) if s is even (odd). Recall that if $\mathcal{V} = \{p^2 : p \text{ prime}\}$, we have $\mathfrak{S}_{k,s,\mathcal{V}}(N) = \mathfrak{S}_{k,s,\mu^2}(N) > 0$ if $k \geq 3$ or Condition A holds. However, if we restrict \mathcal{V} to be a set of prime powers, we are able to determinate whether that $\mathfrak{S}_{\mathcal{V}}(N) > 0$. In this case we write

$$(8) \quad \mathcal{W} =: \{p^{e_p} \mid p \in \mathcal{P}\},$$

instead of \mathcal{V} , where \mathcal{P} is a subset of the prime numbers and (e_p) is a sequence of positive integers. Recall that we assume that there is some $\delta > 0$ such that

$$(9) \quad \sum_{p \in \mathcal{P}} \frac{1}{(p^{e_p})^{1-\delta}} < \infty.$$

Without loss of generality, we can restrict ourselves to the case that $e_p \in \{1, 2\}$ for all $p^{e_p} \in \mathcal{W}$, since a solution with the variables not divisible by p^2 implies a solution with the variables not divisible by p^r with $r \geq 2$.

Next, we define a condition that is necessary for $\mathfrak{S}_{k,s,\mathcal{W}}(N) > 0$ to hold. We define τ by $p^\tau \parallel k$ and let $\sigma := \tau + 1$ if $p \neq 2$ and $\sigma := \tau + 2$ if $p = 2$. For an integer N , we say that (\mathcal{W}, N) satisfies Condition C if the following two conditions hold:

- For each prime p such that $p \in \mathcal{W}$ (i.e. $e_p = 1$) with $p \leq (k-1)^4 + 8k$ there is a solution of

$$x_1^k + \dots + x_s^k \equiv N \pmod{p^\sigma}$$
 with $p \nmid x_1 \cdots x_s$.
- If $k = 2$ and $4 \in \mathcal{W}$, there is a solution of

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv N - 1 \pmod{8}$$
 such that $4 \nmid x_i$ for $i = 1, 2, 3, 4$.

In [6], we showed that for any set of prime powers \mathcal{W} that is defined by (8) such that there is some $\delta > 0$ such that (9) and Condition C hold, we have

$$\mathfrak{S}_{k,s,\mathcal{W}}(N) > 0.$$

One consequence of this results is formula (5) above. For another example, let $k = 2$. In this case, we have to verify Condition C for $p \leq 17$ by an easy computation We get the following result:

Let \mathcal{P} be a set of prime numbers and assume that there is some some $\delta > 0$ such that

$$\sum_{p \in \mathcal{P}} \frac{1}{p^{1-\delta}}$$

converges. Let $N \in \mathbb{N}$ and assume $N \equiv 5 \pmod{8}$ if $2 \in \mathcal{P}$ and $N \equiv 2 \pmod{3}$ if $3 \in \mathcal{P}$. If N is sufficiently large, it can be represented as a sum of five squares of integers not being divisible by any prime of \mathcal{P} .

1.2. Waring's Problem with digital restrictions

Thuswaldner and Tichy [9] investigated Waring's Problem where the digit sums of the variables x_j ($j = 1, \dots, s$) are assumed to be in a certain residue class. Denote by $R_{k,s,h,m}(N)$ the number of solutions of (3) where for all $j = 1, \dots, s$, the variables x_j are assumed to fulfill

$$s_q(x_j) \equiv h \pmod{m}$$

for given integers h, m, q with $m, q \geq 2$ and $(q-1, m) = 1$.

For $s > 2^k$, Thuswaldner and Tichy proved that

$$(10) \quad R_{k,s,h,m}(N) \sim \frac{1}{m^s} R_{k,s}(N)$$

holds. Therefore, the condition that an s -tuple of integers is a solution of (3) is asymptotically in a first-order approximation independent from the condition that its elements fulfill (2). This result has been extended by Pfeiffer and Thuswaldner [8].

1.3. Main result

In the present paper we want to show that one can combine the results presented in Subsec. 1.1 and 1.2. We prove that among the solutions of (3), the conditions $\chi_{\mathcal{V}}(n) = 1$ and (2) are independent. We further show that (3), for sufficient large N and under mild conditions, has a solution where the variables meet $\chi_{\mathcal{V}}(n) = 1$ and (2).

Theorem 1. *Let $s, k \in \mathbb{N}$ with $s > 2^k$, $h_j, m_j, q_j \in \mathbb{N}$ satisfying $(q_j - 1, m_j) = 1$, for all $j = 1, \dots, s$. Let \mathcal{V} be a set of pairwise coprime integers not containing 1 and assume that there is some $\delta > 0$ such that (6) is finite. Let $R_{k,s,\mathbf{h},\mathbf{m},\mathcal{V}}(N)$ be the number of solutions of (3) with*

$$v \nmid x_j \quad \forall v \in \mathcal{V}$$

and

$$s_{q_j}(x_j) \equiv h_j \pmod{m_j}$$

for all $j = 1, \dots, s$. Then the asymptotic formula

$$(11) \quad R_{k,s,\mathbf{h},\mathbf{m},\mathcal{V}}(N) = \frac{1}{m_1 \cdots m_s} \mathfrak{S}_{k,s,\mathcal{V}}(N) N^{s/k-1} + O\left(\frac{N^{s/k-1}}{(\log \log N)^A}\right)$$

holds for all non negative $A \in \mathbb{R}$.

The constants implied by the use of the symbols O and \ll in this paper may depend on k, s, A , the set \mathcal{V} , δ and on q_j, m_j for all $j = 1, \dots, s$. Recall that in Subsec. 1.1 we discussed the positivity of $\mathfrak{S}_{k,s,\mathcal{V}}(N)$.

Our method of proof does not permit the derivation of a better error term (see Rem. 2 at the end of Sec. 2). Although the condition $s > 2^k$ can be weakened as in the classical Waring's Problem if one only assumes that the variables meet (2), the assumption $s > 2^k$ is essential in the proof of Th. 1 (see Rem. 1 after Lemma 1).

2. Preliminaries and the circle method

First, we need some results concerning the notion of our set \mathcal{V} . For details, we refer to [5]. We define

$$\Pi(\mathcal{V}) := \left\{ n = \prod_{v \in \mathcal{V}'} v : \mathcal{V}' \text{ is a finite subset of } \mathcal{V} \right\}$$

and

$$\mu_{\mathcal{V}}(n) := \begin{cases} (-1)^{\#\mathcal{V}'} & \text{if } n \in \Pi(\mathcal{V}) \text{ with } n = \prod_{v \in \mathcal{V}'} v, \\ 0 & \text{otherwise,} \end{cases}$$

a variant of the well known Möbius μ -function. Notice that $1 \in \Pi(\mathcal{V})$, since we define the empty product as 1. Similarly to $\mu^2(n) = \sum_{d^2|n} \mu(n)$, the convolution formula

$$(12) \quad \chi_{\mathcal{V}}(n) = \sum_{\substack{m \in \Pi(\mathcal{V}) \\ m|n}} \mu_{\mathcal{V}}(m)$$

holds and is easy to verify. Besides, as (6) is finite, one has

$$(13) \quad \sum_{\substack{d > Y \\ d \in \Pi(\mathcal{V})}} \frac{1}{d} \ll Y^{-\delta}.$$

Now, we apply the circle method. We fix $A \in \mathbb{R}$ arbitrarily large. Thus

$$(14) \quad R_{k,s,\mathbf{h},\mathbf{m},\mathcal{V}}(N) = \int_0^1 \left(\prod_{i=1}^s u_i(P, \theta) \right) e(-N\theta) d\theta,$$

where we define

$$u_i(P, \theta) := \sum_{\substack{n_i < P \\ s_{q_i}(n_i) \equiv h_i \pmod{m_i}}} \chi_{\mathcal{V}}(n_i) e(n_i^k \theta)$$

and $P := \lfloor N^{1/k} \rfloor$. As usual, $e(\theta)$ stands for $e^{2\pi i \theta}$. In order to remove the congruence condition $s_{q_i}(n_i) \equiv h_i \pmod{m_i}$ in $u_i(P, \theta)$, we write

$$u_i(P, \theta) = \frac{1}{m_i} \sum_{l=0}^{m_i-1} \sum_{n < P} \chi_{\mathcal{V}}(n) e\left(l \frac{s_{q_i}(n) - h_i}{m_i} \right) e(\theta n_i^k)$$

by following Gelfond [4]. We insert this into (14) and split the obtained expression into a part where all $l_i = 0$ ($i = 1, \dots, s$) and a remaining part. This yields

$$(15) \quad \begin{aligned} R_{k,s,\mathbf{h},\mathbf{m},\mathcal{V}}(N) &= \\ &= \frac{1}{m_1 \cdots m_s} \int_0^1 \sum_{n_1 < P} \chi_{\mathcal{V}}(n_1) \cdots \sum_{n_s < P} \chi_{\mathcal{V}}(n_s) e(\theta (n_1^k + \cdots + n_s^k - N)) d\theta + \\ &+ \frac{1}{m_1 \cdots m_s} \underbrace{\sum_{l_1=0}^{m_1-1} \cdots \sum_{l_s=0}^{m_s-1}}_{l_1 + \cdots + l_s \neq 0} \int_0^1 \left(\prod_{i=1}^s S_{i,l_i}(P, \theta) \right) e(-N\theta) d\theta \end{aligned}$$

with

$$S_{i,l_i}(P, \theta) := \sum_{n_i < P} e \left(\theta n_i^k + l_i \frac{s_{q_i}(n) - h_i}{m_i} \right) \chi_{\mathcal{V}}(n_i).$$

Note that the first integral in (15) equals $R_{k,s,\mathcal{V}}(N)$ and we can utilize (7).

Let $\mathbf{l} := (l_1, \dots, l_s)$ with $0 \leq l_i \leq m_i - 1$ ($i = 1, \dots, s$) and $l_1 + \dots + l_s \neq 0$, and we define

$$L_{\mathbf{l}} := \int_0^1 \left(\prod_{i=1}^s S_{i,l_i}(P, \theta) \right) e(-N\theta) d\theta.$$

Th. 1 follows if we prove that $L_{\mathbf{l}} = O(N^{s/k-1}/(\log \log N)^A)$. Let l_j be an entry of \mathbf{l} that is not equal to 0. Then

$$(16) \quad |L_{\mathbf{l}}| \leq \sup_{\theta \in [0,1]} \left\{ |S_{j,l_j}(P, \theta)| \right\} \max_{i \in \{1, \dots, s\}} \left\{ \int_0^1 |S_{i,l_i}(P, \theta)|^{s-1} d\theta \right\}.$$

Since $s > 2^k$, we have

$$\begin{aligned} & \int_0^1 |S_{i,l_i}(P, \theta)|^{s-1} d\theta \leq \\ & \leq P^{s-1-2^k} \int_0^1 S_{i,l_i}(P, \theta)^{2^{(k-1)}} \overline{S_{i,l_i}(P, \theta)^{2^{(k-1)}}} d\theta \leq \\ & \leq P^{s-1-2^k} \# \{n_1, \dots, n_s < P : n_1^k + \dots + n_{2^{k-1}}^k = n_{2^{k-1}-1}^k + \dots + n_{2^k}^k\} \ll \\ & \ll P^{s-k-1}, \end{aligned}$$

where we utilized Vaughan [11, Th. 2], a strong version of Hua's Lemma. We deduce from (16) that

$$L_{\mathbf{l}} = O \left(\sup_{\theta \in [0,1]} \left\{ |S_{j,l_j}(P, \theta)^{s-2^k}| \right\} P^{s-k-1} \right).$$

Hence, the following lemma yields Th. 1.

Lemma 1. *Let l, m, k, q be positive integers with $m \geq 2, q \geq 2$ and $m \nmid l(q-1)$. Then*

$$S(N) := \sum_{n < N} e \left(\theta n^k + \frac{l}{m} s_q(n) \right) \chi_{\mathcal{V}}(n) \ll \frac{N}{(\log \log N)^A}$$

holds uniformly in $\theta \in [0, 1)$.

Remark 1. Above, we made use of Vaughan [11, Th. 2] where the condition $s > 2^k$ is necessary. If $s > 2^k$ does not hold, relevant version's of Hua's Lemma imply an additional factor P^ε for an upper bound which

is too big since we can not improve the bound $S(N) \ll N/(\log \log N)^A$ in Lemma 1.

Applying the convolution formula (12), we have

$$(17) \quad S(N) = \sum_{\substack{d \geq 1 \\ d \in \Pi(\mathcal{V})}} \mu_{\mathcal{V}}(d) \sum_{n < N/d} e\left(z^k \theta n^k + \frac{l}{m} s_q(nd)\right).$$

Let $T := A/\delta$. We split up the sum into two parts with $d \geq (\log \log N)^T$ and $d < (\log \log N)^T$. Therefore

$$\begin{aligned} S(N) &\ll \sum_{\substack{d \geq (\log \log N)^T \\ d \in \Pi(\mathcal{V})}} \frac{N}{d} + \sum_{\substack{d < (\log \log N)^T \\ d \in \Pi(\mathcal{V})}} |\mu_{\mathcal{V}}(d)| \left| \sum_{n < N/d} e\left(d^k \theta n^k + \frac{l}{m} s_q(nd)\right) \right| \ll \\ &\ll \frac{N}{(\log \log N)^A} + \\ &\quad + (\log \log N)^T \max_{\substack{d < (\log \log N)^T \\ d \in \Pi(\mathcal{V})}} \left\{ \left| \sum_{n < N/d} e\left(d^k \theta n^k + \frac{l}{m} s_q(nd)\right) \right| \right\}, \end{aligned}$$

by using (6).

Theorem 2. *Let $B, D > 0$ and let $q, d \in \mathbb{N}$. Then one has*

$$\sum_{n < N/d} e\left(\theta n^k + \frac{l}{m} s_q(nd)\right) \ll \frac{N}{(\log N)^B}$$

uniformly for $\theta \in \mathbb{R}$ and $d \leq (\log \log N)^D$.

Th. 1 is proved by applying Th. 2 with $D = T$. Notice that $N(\log \log N)^{2A}/(\log N)^B \ll N/(\log \log N)^A$. The proof of Th. 2 is the objective of the remaining paper.

Remark 2. The bound of Th. 2 is stronger than necessary. However, we can not achieve a better error term in Th. 1 since the condition $d \leq (\log \log N)^D$ in Th. 2 is necessary and forces us to bound the summands in (17) with $d \geq (\log \log N)^T$ trivially by N/d . Therefore, we are not able to improve the error term $O(N^{s/k-1}/(\log \log N)^A)$ in (11).

3. Weyl's inequality

Let $k \in \mathbb{N}$, $\rho : \mathbb{N} \rightarrow \mathbb{C}$ and $n, h_1, h_2, \dots \in \mathbb{N}$. We define the higher difference operators Δ_k recursively by

$$\Delta_1(\rho(n); h_1) := \rho(n + h_1) - \rho(n)$$

and

$$\Delta_{j+1} := \Delta_1(\Delta_j(\rho(n); h_1, \dots, h_j); h_{j+1})$$

for $j \in \mathbb{N}$. Notice that $\Delta_k(n^k; h_1, \dots, h_k)$ is independent on n .

We define $I \subseteq \mathbb{N}$ to be an interval of integers if $I := \{n \in \mathbb{N} : a \leq n < b\}$ for certain $a, b \in \mathbb{N}$. The aim of this section is to show that the following proposition implies Th. 2.

Proposition 1. *Let $B, D > 0$ and let d, k, m, h, q, N be positive integers such that $m \geq 2$, $q \geq 2$ and $m \nmid h(q-1)$. Let further U_1, \dots, U_k, J be intervals of integers with $\sqrt{N}/d < |U_i|$ for all $i = 1, \dots, k$. Assume $|J| \leq N$. We further define*

$$Y(U_1, \dots, U_k, J) := \sum_{h_1 \in U_1} \cdots \sum_{h_k \in U_k} \left| \sum_{n \in J} e\left(\frac{h}{m} \Delta_k(s_q(dn); h_1, \dots, h_k)\right) \right|^2.$$

Then

$$Y(U_1, \dots, U_k, J) \ll |U_1| \cdots |U_k| |J|^2 \frac{1}{(\log N)^B}$$

holds uniformly for all $d \leq (\log \log N)^D$.

We can argue literally as in Sec. 8 of [9] to prove that Th. 2 can be deduced from Prop. 1. Therefore, we only give a short sketch of this statement.

Proof of (Prop. 1 \Rightarrow Th. 2). For abbreviation, let $M := \lfloor N/d \rfloor$. Using the classical version of Weyl's Lemma (see e.g. [10, Lemma 2.3]), we get

$$\begin{aligned} & \left| \sum_{n < M} e\left(\theta n^k + \frac{l}{m} s_q(dn)\right) \right|^{2^k} \leq \\ & \leq (2M)^{2^k - k - 1} \sum_{|h_1|, \dots, |h_k| < M} \left| \sum_{n \in H_k(h_1, \dots, h_k)} e\left(\frac{l}{m} \Delta_k(s_q(dn); h_1, \dots, h_k)\right) \right|, \end{aligned}$$

where $H_k(h_1, \dots, h_k)$ is an interval of integers depending linearly on h_1, \dots, h_k . We remove this dependence by splitting up the sums into parts of reasonable size. Besides, we make use of the Cauchy–Schwarz inequality in order to get a square of the modulus of the innermost sum. Now, we can apply Prop. 1. \diamond

Remark 3. Prop. 1 follows from Th. 3.4 of [9] in the case of $d = 1$. Thus it suffices to prove Prop. 1 for $2 \leq d \leq (\log \log N)^D$.

4. Auto-correlation functions

Let d always denote an integer with $2 \leq d \leq (\log \log N)^D$. Let

$$\mathcal{Q} := \{0, 1, 2, \dots, q-1\},$$

$$M := \{1, 2, \dots, k\},$$

$$M' := \{0, 1, 2, \dots, k+d\},$$

and

$$\mathcal{F} := \{f : \mathcal{P}(M) \rightarrow M'\},$$

where $\mathcal{P}(M)$ denotes the set of all subsets of M . For $\mathbf{r} = (r_1, r_2, \dots, r_k) \in \mathcal{Q}^k$, $i \in \mathcal{Q}$ and $S \subseteq M$ we define

$$\Xi_{\mathbf{r},i}(f)(S) := \left[di + \sum_{t \in S} r_t + f(S) \right]_q,$$

with $[x]_q := \lfloor x/q \rfloor$. Notice that $f \in \mathcal{F}$ implies $\Xi_{\mathbf{r},i}(f) \in \mathcal{F}$. Let $F_0, F_1 \in \mathcal{F}$ be defined by

$$F_0(S) := 0$$

for all $S \subseteq M$ and

$$F_1(M) := 1, \quad F_1(S) := 0$$

for all $S \subsetneq M$. Further, we define iterates of $\Xi_{\mathbf{r},i}$ by

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

where the composition is defined by

$$(\Xi_{\mathbf{r}_2, i_2} \circ \Xi_{\mathbf{r}_1, i_1})(f)(S) := \Xi_{\mathbf{r}_2, i_2}(\Xi_{\mathbf{r}_1, i_1}(f))(S)$$

for $f \in \mathcal{F}$, $S \subseteq M$. For the sake of a simple notation, let $\Xi_{\{\mathbf{r}_\ell, i_\ell\}_{\ell \in \emptyset}}(f) := f$, where \emptyset denotes the empty set.

Let $L \in \mathbb{N}$, $\ell \leq L$ and $\mathbf{r}_\ell \in \mathcal{Q}^k$, $i_{\ell 1}, i_{\ell 2} \in \mathcal{Q}$. Let further $f_1, f_2, g_1, g_2 \in \mathcal{F}$. We define

$$(f_1, f_2) \xrightarrow{(\mathbf{r}_\ell, i_{\ell 1}, i_{\ell 2})_{1 \leq \ell \leq L}} (g_1, g_2)$$

to be an equivalent expression for

$$\Xi_{\{\mathbf{r}_\ell, i_{\ell 1}\}_{1 \leq \ell \leq L}}(f_1) = g_1 \quad \wedge \quad \Xi_{\{\mathbf{r}_\ell, i_{\ell 2}\}_{1 \leq \ell \leq L}}(f_2) = g_2.$$

Lemma 2. *There is a sequence $(\hat{\mathbf{r}}_\ell, \hat{i}_{\ell 1}, \hat{i}_{\ell 2})_{1 \leq \ell \leq L'}$ with $L' \leq \frac{\log(d(k+d))}{\log q} + k + 2$ such that for any $(f_1, f_2) \in \mathcal{F}^2$ one has*

$$(f_1, f_2) \xrightarrow{(\hat{\mathbf{r}}_\ell, \hat{i}_{\ell 1}, \hat{i}_{\ell 2})_{1 \leq \ell \leq L'}} (F_1, F_0).$$

We denote such a sequence a (F_1, F_0) -sequence with length L' .

Proof. The (F_1, F_0) -sequence can be thus constructed by a composition of three sequences that are defined below.

First, it is easy to see that

$$(18) \quad (f_1, f_2) \xrightarrow{(\mathbf{0}, 0, 0)_{1 \leq \ell \leq L_1}} (F_0, F_0)$$

holds for $L_1 = \lfloor \log(k+d)/\log q \rfloor + 1$.

Given a sequence $(\mathbf{r}_\ell, i_{\ell 1}, i_{\ell 2})_{1 \leq \ell \leq L}$, we define $G_1, H_1, G_2, H_2, \dots \in \mathcal{F}$ such that

$$(F_0, F_0) \xrightarrow{(\mathbf{r}_1, i_{11}, i_{12})} (G_1, H_1) \xrightarrow{(\mathbf{r}_2, i_{21}, i_{22})} (G_2, H_2) \xrightarrow{(\mathbf{r}_3, i_{31}, i_{32})} (G_3, H_3) \ddots \dots$$

holds.

For $1 \leq \beta \leq q-1$, let $\beta^* \in \mathcal{F}$ be defined by

$$\beta^*(S) := \beta$$

for all $S \subseteq M$. We show that there is an integer $1 \leq \beta \leq q-1$ and a sequence $(\mathbf{r}_\ell, i_{\ell 1}, i_{\ell 2})_{1 \leq \ell \leq L_2}$ with

$$(19) \quad (F_0, F_0) \xrightarrow{(\mathbf{r}_\ell, i_{\ell 1}, i_{\ell 2})_{1 \leq \ell \leq L_2}} (\beta^*, F_0)$$

and $L_2 \leq \log d / \log q + 1$.

Recall that we can assume $d \geq 2$ by Rem. 3. If $2 \leq d < q$, we set $i_{11} = q-1, i_{12} = 0$ and $\mathbf{r}_1 = (0, \dots, 0)$. Thus

$$1 \leq G_1(S) = \lfloor d(q-1) \rfloor_q \leq q-1$$

since $2 \leq d \leq q-1$ and $G_1(S)$ is independent on S . Clearly, we have

$$H_1(S) = F_0(S)$$

for all $S \subseteq M$. We take $L_2 := 1$ and $\beta := G_1(S)$ and the sequence in (19) is constructed.

Now, we assume that $d \geq q$. We take $i_{11} = 1, i_{12} = 0$ and $\mathbf{r}_1 = (0, \dots, 0)$. Hence

$$G_1(S) = \lfloor d \rfloor_q = \alpha_1,$$

where $\alpha_1 \in \mathbb{N}$ is defined via $d = q\alpha_1 + \beta_1$ with $\beta_1 \in \mathcal{Q}$. Again, we have $H_1 = F_0$. Notice that $\alpha_1 > 0$ by our assumption $d \geq q$. If $\alpha_1 \in \mathcal{Q}$ we take $L_2 := 1$ and $H_1 = \beta^*$ with $\beta = \alpha_1$. Besides, let $J \in \mathbb{N}$. For all $2 \leq j \leq J$ we take $i_{j1} := i_{j2} := 0$ and $\mathbf{r}_j = (0, \dots, 0)$. Since $\mathbf{r}_j = (0, \dots, 0)$ the value of $G_j(S)$ and $H_j(S)$ is independent on S . Now, we have $H_j(S) = F_0$ and $0 \leq G_j(S) < G_{j-1}(S)$ for all $2 \leq j \leq J$. We take $L_2 \in \{2, 3, 4, \dots\}$ minimal such that $G_{L_2}(S) \in \mathcal{Q}$ for the first time. Notice that we have $G_{L_2}(S) > 0$. For if

$$0 = G_{L_2} J(S) = \lfloor G_{L_2-1}(S) \rfloor_q$$

we have $G_{L_2-1} \in \mathcal{Q}$ and this contradicts the minimality of L_2 . We define $\beta := G_{L_2}(S) = \beta^*(S)$. Notice that $L_2 \leq \log d / \log q + 1$.

Given a sequence $(\mathbf{r}_\ell, i_{\ell 1}, i_{\ell 2})_{1 \leq \ell \leq L}$ let $\tilde{G}_1, \tilde{H}_1, \tilde{G}_2, \tilde{H}_2, \dots \in \mathcal{F}$ be defined via

$$(\beta^*, F_0) \xrightarrow{(\mathbf{r}_1, i_{11}, i_{12})} (\tilde{G}_1, \tilde{H}_1) \xrightarrow{(\mathbf{r}_2, i_{21}, i_{22})} (\tilde{G}_2, \tilde{H}_2) \xrightarrow{(\mathbf{r}_3, i_{31}, i_{32})} (\tilde{G}_3, \tilde{H}_3) \rightsquigarrow \dots$$

Finally, we construct a sequence $(\mathbf{r}_\ell, i_{\ell 1}, i_{\ell 2})_{1 \leq \ell \leq k}$ with

$$(20) \quad (\beta^*, F_0) \xrightarrow{(\mathbf{r}_\ell, i_{\ell 1}, i_{\ell 2})_{1 \leq \ell \leq k}} (F_1, F_0).$$

For $1 \leq \ell \leq k$ we take $i_{1\ell} := i_{2\ell} := 0$ and let

$$\mathbf{r}_1 := (q - \beta, 0, 0, \dots, 0).$$

Recall that $1 \leq \beta \leq q - 1$. Hence

$$\tilde{G}_1(S) = \left[\sum_{t \in S} r_t + \beta \right]_q = \begin{cases} 1 & \text{if } 1 \in S, \\ 0 & \text{otherwise} \end{cases}$$

and

$$\tilde{H}_1(S) = \left[\sum_{t \in S} r_t \right]_q = F_0(S)$$

Let $\mathbf{r}_2 := (0, q - 1, 0, 0, \dots, 0)$. Thus

$$\tilde{G}_2(S) = \left[\sum_{t \in S} r_t + \tilde{G}_1(S) \right]_q = \begin{cases} 1 & \text{if } 1, 2 \in S, \\ 0 & \text{otherwise} \end{cases}$$

and $\tilde{H}_2 = F_0$. In this manner, let

$$\begin{aligned} \mathbf{r}_3 &:= (0, 0, q - 1, 0, \dots, 0) \\ \mathbf{r}_4 &:= (0, 0, 0, q - 1, \dots, 0) \\ &\vdots \\ \mathbf{r}_{k-1} &:= (0, 0, 0, 0, \dots, 0, q - 1, 0) \\ \mathbf{r}_k &:= (0, 0, 0, 0, \dots, 0, q - 1). \end{aligned}$$

Hence

$$\tilde{G}_\ell(S) = \left[\sum_{t \in S} r_t + \tilde{G}_{\ell-1}(S) \right]_q = \begin{cases} 1 & \text{if } 1, 2, \dots, \ell \in S, \\ 0 & \text{otherwise} \end{cases}$$

and $\tilde{H}_\ell = F_0$ for all $1 \leq \ell \leq k$. Thus we have $\tilde{G}_k = F_1$ and $\tilde{H}_k = F_0$. The lemma follows from (18), (19), and (20). \diamond

Let

$$(21) \quad \mathbf{r}^* := (q - k, 1, 1, 1, \dots, 1) \in \mathcal{Q}^k.$$

Notice that the sum of the entries of \mathbf{r}^* equals $q - 1$. Thus, the equations

$$(22) \quad \begin{aligned} \Xi_{(\mathbf{r}^*, 0)}(F_0) &= F_0, \\ \Xi_{(\mathbf{r}^*, 0)}(F_1) &= F_1, \\ \Xi_{(\mathbf{0}, 0)}(F_1) &= F_0, \\ \Xi_{(\mathbf{0}, 0)}(F_0) &= F_0 \end{aligned}$$

are easily proved. Let

$$(23) \quad L := L' + 2,$$

where L' is as in Lemma 2.

We define two sequences

$$\mathcal{V}_1 = (\mathbf{r}_l, i_{l1}, i_{l2})_{1 \leq l \leq L} \quad \text{and} \quad \mathcal{V}_2 = (\tilde{\mathbf{r}}_l, \tilde{i}_{l1}, \tilde{i}_{l2})_{1 \leq l \leq L}$$

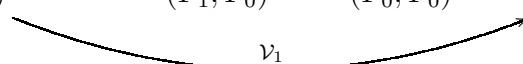
that play an important role in the proof of Th. 1: for $1 \leq l \leq L'$ let

$$\begin{aligned} (\mathbf{r}_l, i_{l1}, i_{l2}) &:= (\hat{\mathbf{r}}_l, \hat{i}_{l1}, \hat{i}_{l2}) \quad \text{and} \\ (\tilde{\mathbf{r}}_l, \tilde{i}_{l1}, \tilde{i}_{l2}) &:= (\hat{\mathbf{r}}_l, \hat{i}_{l1}, \hat{i}_{l2}), \end{aligned}$$

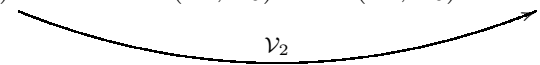
where $(\hat{\mathbf{r}}_l, \hat{i}_{l1}, \hat{i}_{l2})$ are the entries of the (F_1, F_0) -sequence with length L' defined in Lemma 2. Let further

$$(24) \quad \begin{aligned} \mathbf{r}_l &:= (0, 0, \dots, 0), \quad \tilde{\mathbf{r}}_l := \mathbf{r}^* \quad \text{for } l = L - 1, \\ \mathbf{r}_l = \tilde{\mathbf{r}}_l &:= (0, 0, \dots, 0) \quad \text{for } l = L, \\ i_{l1} = i_{l2} = \tilde{i}_{l1} = \tilde{i}_{l2} &:= 0 \quad \text{for } l = L - 1 \text{ or } l = L. \end{aligned}$$

Thus we conclude by (22) and Lemma 2 that

$$(25) \quad (f_1, f_2) \xrightarrow{(F_1, F_0)\text{-sequence}} (F_1, F_0) \xrightarrow{(\mathbf{0}, 0, 0)} (F_0, F_0) \xrightarrow{(\mathbf{0}, 0, 0)} (F_0, F_0)$$


and

$$(26) \quad (f_1, f_2) \xrightarrow{(F_1, F_0)\text{-sequence}} (F_1, F_0) \xrightarrow{(\mathbf{r}^*, 0, 0)} (F_1, F_0) \xrightarrow{(\mathbf{0}, 0, 0)} (F_0, F_0)$$


holds for all $(f_1, f_2) \in \mathcal{F}^2$.

Later, the following lemma will be of use. Its proof is straightforward.

Lemma 3. *Let G be a finite set and $A := (a_{ij})_{i,j \in G}$ be a matrix with non negative real entries. For $y \in \mathbb{N}$, let $(a_{ij}^{(y)})_{i,j \in G} := A^y$. Let $X > 0$ with $\sum_{k \in G} a_{ik} \leq X$, for all $i \in G$. One has*

$$\sum_{k \in G} a_{ik}^{(y)} \leq X^y$$

for all $i \in G$.

5. Iterations

Recall that our aim is to show Prop. 1. Let $B, D > 0$ and $2 \leq d \leq (\log \log N)^D$.

Let I be an interval of integers, i.e. $I := \{n \in \mathbb{N} : a \leq n < b\}$ for certain integers $a < b$. For $c \in \mathbb{N}$ we define $cI := \{n \in \mathbb{N} : ca \leq n < cb\}$. For $f_1, f_2 \in \mathcal{F}$ and I_1, \dots, I_k, J intervals of integers let

$$\Phi(h_1, \dots, h_k; J, f_1) := \sum_{n \in J} e\left(\frac{h}{m} \sum_{S \subseteq M} (-1)^{k-|S|} s_q \left(dn + \sum_{t \in S} h_t + f_1(S) \right)\right).$$

We further define

$$\Psi(I_1, \dots, I_{k-1}; I_k, J, f_1, f_2) := \sum_{h_k \in I_k} \overline{\Phi(h_1, \dots, h_k; J, f_1)} \Phi(h_1, \dots, h_k; J, f_2)$$

and

$$X(I_1, \dots, I_k; J, f_1, f_2) := \sum_{h_1 \in I_1} \cdots \sum_{h_{k-1} \in I_{k-1}} \Psi(h_1, \dots, h_{k-1}; I_k, J, f_1, f_2).$$

Since

$$\Delta_k(s_q(dn), h_1, \dots, h_k) = \sum_{S \subseteq M} (-1)^{k-|S|} s_q \left(dn + \sum_{t \in S} dh_t \right),$$

we have

$$\begin{aligned}
Y(U_1, \dots, U_k, J) &= \\
&= \sum_{h_1 \in U_1} \cdots \sum_{h_k \in U_k} \left| \sum_{n \in J} e \left(\frac{h}{m} \sum_{S \subseteq M} (-1)^{k-|S|} s_q \left(dn + \sum_{t \in S} dh_t \right) \right) \right|^2 \leq \\
&\leq \sum_{h_1 \in dU_1} \cdots \sum_{h_k \in dU_k} \left| \sum_{n \in J} e \left(\frac{h}{m} \sum_{S \subseteq M} (-1)^{k-|S|} s_q \left(dn + \sum_{t \in S} h_t \right) \right) \right|^2 = \\
&= X(I_1, \dots, I_k; J, F_0, F_0),
\end{aligned}$$

where $I_i := dU_i$. Thus $\sqrt{N} < |I_i|$. Note that we substitute in the inner sum dh_i by h_i since we extend the intervals U_i to $I_i = dU_i$. This is the essential trick of this paper. Our aim is now to show

$$(27) \quad X(I_1, \dots, I_k; J, f_1, f_2) \ll |I_1| \cdots |I_k| |J|^2 \frac{1}{(\log N)^{2B}}$$

for arbitrary $f_1, f_2 \in \mathcal{F}$,

$$(28) \quad \sqrt{N} < |I_i| \quad \text{and} \quad |J| \leq N.$$

Recall that $d \leq (\log \log N)^D$. Provided that we can show (27), we take $f_1, f_2 = F_0$ and obtain

$$\begin{aligned}
Y(U_1, \dots, U_k, J) &\leq X(I_1, \dots, I_k; J, F_0, F_0) \ll \\
&\ll |I_1| \cdots |I_k| |J|^2 \frac{1}{(\log N)^{2B}} \ll \\
&\ll |U_1| \cdots |U_k| |J|^2 (\log \log N)^{kD} \frac{1}{(\log N)^{2B}} \ll \\
&\ll |U_1| \cdots |U_k| |J|^2 \frac{1}{(\log N)^B}.
\end{aligned}$$

Thus, to prove Prop. 1 and consequently to prove Th. 1, it suffices to show (27), which is the matter of the remaining paper. To do so, we need the following technical lemma which is similar to [9, Prop. 5.1].

Lemma 4. *For $f_1, f_2 \in \mathcal{F}$, $L \in \mathbb{N}$ we have*

$$\begin{aligned}
(29) \quad X(q^L I_1, \dots, q^L I_k; q^L J, f_1, f_2) &= \\
&= \sum_{\mathbf{r}_1, \dots, \mathbf{r}_L \in \mathcal{Q}^k} \sum_{\mathbf{i}_1, \dots, \mathbf{i}_L \in \mathcal{Q}^2} \\
&\quad \prod_{\ell=1}^L \alpha \left(\Xi_{\{\mathbf{r}_j, i_{j1}\}_{1 \leq j \leq \ell-1}}(f_1), \Xi_{\{\mathbf{r}_j, i_{j2}\}_{1 \leq j \leq \ell-1}}(f_2), \mathbf{r}_\ell, i_{\ell 1}, i_{\ell 2} \right) \\
&\quad X(I_1, \dots, I_k, J; \Xi_{\{\mathbf{r}_1, i_{\ell 1}\}_{1 \leq \ell \leq L}}, \Xi_{\{\mathbf{r}_1, i_{\ell 2}\}_{1 \leq \ell \leq L}}(f_1)),
\end{aligned}$$

where

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

and $b(f, S, \mathbf{r}, i) \in \mathcal{Q}$ is defined via

$$di + \sum_{t \in S} r_t + f(S) = zq + b(f, S, \mathbf{r}, i)$$

with $z \in \mathbb{N}$.

Remark 4. Note that $z = \Xi_{\mathbf{r},i}(f)(S) = \lfloor di + \sum_{t \in S} r_t + f(S) \rfloor_q$.

Proof. Note that for an interval of integers I , we have

$$qI = \{qh + r : h \in I, r \in \mathcal{Q}\}.$$

We first prove the case $L = 1$. Therefore, we consider

$$\begin{aligned} & \Phi(qh_1 + r_1, \dots, qh_k + r_k; qJ, f_1) = \\ & = \sum_{i \in \mathcal{Q}} \sum_{n \in J} e \left(\frac{h}{m} \sum_{S \subseteq M} (-1)^{k-|S|} s_q \left(q \left(dn + \sum_{t \in S} h_t \right) + di + \sum_{t \in S} r_t + f_1(S) \right) \right). \end{aligned}$$

Since

$$di + \sum_{t \in S} r_t + f_1(S) = q\Xi_{\mathbf{r},i}(f_1)(S) + b(f_1, S, \mathbf{r}, i),$$

we get due to the q -additivity of the sum-of-digits function

$$\begin{aligned} & s_q \left(q \left(dn + \sum_{t \in S} h_t \right) + di + \sum_{t \in S} r_t + f_1(S) \right) = \\ & = s_q \left(dn + \sum_{t \in S} h_t + \Xi_{\mathbf{r},i}(f_1)(S) \right) + b(f_1, S, \mathbf{r}, i). \end{aligned}$$

By the definition of $X(I_1, \dots, I_k; J, f_1, f_2)$, the lemma is proved in the case $L = 1$. Repeating the procedure $L - 1$ times yields the result. \diamond

Lemma 5. One has

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

where \mathbf{r}^* is defined in (21).

Proof. Let

$$\Upsilon_{\mathbf{r},i}(f)(S) := di + \sum_{t \in S} r_t + f(S).$$

The remainder occurring at the division of $\Upsilon_{\mathbf{r},i}(f)(S)$ by q is $b(f, S, \mathbf{r}, i)$. Since $\Upsilon_{\mathbf{0},0}(F_0)(S) = 0$ for all $S \subseteq M$, the first statement of the lemma is valid. We have further $\Upsilon_{\mathbf{0},0}(F_1)(S) = 0$ for all $S \subsetneq M$ and $\Upsilon_{\mathbf{0},0}(F_1)(M) = 1$, thus $\alpha(F_1, F_0, \mathbf{0}, 0, 0) = e(h/m)$.

It remains to prove the last statement of the lemma. For all $S \subsetneq M$ we have $\Upsilon_{\mathbf{r}^*,0}(F_1)(S) = \Upsilon_{\mathbf{r}^*,0}(F_0)(S)$ and consequently $b(F_1, S, \mathbf{r}^*, 0) = b(F_0, S, \mathbf{r}^*, 0)$. Hence

$$\alpha(F_1, F_0, \mathbf{r}^*, 0, 0) = e \left(\frac{h}{m} (b(F_1, M, \mathbf{r}^*, 0) - b(F_0, M, \mathbf{r}^*, 0)) \right).$$

We have $\Upsilon_{\mathbf{r}^*,0}(F_1)(M) = q$ and $\Upsilon_{\mathbf{r}^*,0}(F_0)(M) = q - 1$. Hence

$$b(F_1, M, \mathbf{r}^*, 0) - b(F_0, M, \mathbf{r}^*, 0) = 1 - q,$$

and the lemma follows. \diamond

Recall that we need to show (27) in order to proof Th. 1.

Lemma 6. *Let $L := L' + 2$, where L' as in Lemma 2. Let further $m \nmid h(q-1)$, and $f_1, f_2 \in \mathcal{F}$. Then the inequality*

$$\begin{aligned} & |X(q^{Lt}I_1, \dots, q^{Lt}I_k, q^{Lt}J; f_1, f_2)| \leq \\ & \leq \left(1 - \frac{\pi^2}{(4m^2q^{(k+2)L})} \right)^t (q^{Lt}|I_1|) \cdots (q^{Lt}|I_k|) (q^{Lt}|J|)^2 \end{aligned}$$

holds for all $t \in \mathbb{N}$.

Proof. We extract two summands V_1 and V_2 from (29) that correspond to the sequences \mathcal{V}_1 and \mathcal{V}_2 respectively defined in (24). Thus Lemma 4 yields

(30)

$$\begin{aligned} & X(q^L I_1, \dots, q^L I_k; q^L J, f_1, f_2) = \\ & = V_1 + V_2 + \sum_{\Gamma} \prod_{\ell=1}^L \alpha(\Xi_{\{\mathbf{r}_j, i_{j1}\}_{1 \leq j \leq \ell-1}}(f_1), \Xi_{\{\mathbf{r}_j, i_{j2}\}_{1 \leq j \leq \ell-1}}(f_2), \mathbf{r}_L, i_{L1}, i_{L2}) \\ & X(I_1, \dots, I_k, J; \Xi_{\{\mathbf{r}_1, i_{\ell 1}\}_{1 \leq \ell \leq L}}, \Xi_{\{\mathbf{r}_1, i_{\ell 2}\}_{1 \leq \ell \leq L}}(f_1)), \end{aligned}$$

where Γ denotes the set off all $(\mathbf{r}_1, \dots, \mathbf{r}_L, \mathbf{i}_1, \dots, \mathbf{i}_L) \in (\mathcal{Q}^k)^L \times (\mathcal{Q}^2)^L$ apart from the two elements corresponding to \mathcal{V}_1 or \mathcal{V}_2 . Thus $|\Gamma| = q^{(k+2)L} - 2$.

We use the abbreviation

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

We obtain by (25) and (26) that

$$V_1 = A(f_1, f_2) \alpha(F_1, F_0, \mathbf{0}, 0, 0) \alpha(F_0, F_0, \mathbf{0}, 0, 0) X(I_1, \dots, I_k, J; F_0, F_0)$$

and

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

By Lemma 5, we thus get

$$V_1 + V_2 = A(f_1, f_2) e \left(\frac{h}{m} \right) \left(1 + e \left((1-q) \frac{h}{m} \right) \right) X(I_1, \dots, I_k, J, F_0, F_0).$$

For given functions $f_1, f_2, g_1, g_2 \in \mathcal{F}$, let E_{f_1, f_2, g_1, g_2} denote the set of all $(\mathbf{r}_1, \dots, \mathbf{r}_L, \mathbf{i}_1, \dots, \mathbf{i}_L) \in \Gamma$ satisfying

$$X(I_1, \dots, I_k, J; \Xi_{\{\mathbf{r}_1, i_{\ell 1}\}_{1 \leq \ell \leq L}}, \Xi_{\{\mathbf{r}_1, i_{\ell 2}\}_{1 \leq \ell \leq L}}(f_1)) = X(I_1, \dots, I_k, J, g_1, g_2).$$

We define

$$a'(f_1, f_2, g_1, g_2) := \sum_{E_{f_1, f_2, g_1, g_2}} \alpha(f_1, f_2, \mathbf{r}, i_1, i_2).$$

Recall that $|\Gamma| = q^{(k+2)L} - 2$. The absolute value of the function α is at most 1. Hence, for all $f_1, f_2 \in \mathcal{F}$ one has

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

We rearrange the sum (30) and get

$$\begin{aligned} & X(q^L I_1, \dots, q^L I_k; q^L J, f_1, f_2) = \\ &= \sum_{(F_0, F_0) \neq (g_1, g_2) \in \mathcal{F}} a'(f_1, f_2, g_1, g_2) X(I_1, \dots, I_k, J, g_1, g_2) + \\ &+ \left(a'(F_0, F_0) + A(f_1, f_2) e \left(\frac{h}{m} \right) \left(1 + e \left((1-q) \frac{h}{m} \right) \right) \right) \\ & X(I_1, \dots, I_k, J, F_0, F_0). \end{aligned}$$

Let

$$a(f_1, f_2, g_1, g_2) := a'(f_1, f_2, g_1, g_2)$$

if $(g_1, g_2) \neq (F_0, F_0)$ and let

$$a(f_1, f_2, F_0, F_0) := a'(f_1, f_2, F_0, F_0) + A(f_1, f_2) e \left(\frac{h}{m} \right) \left(1 + e \left((1-q) \frac{h}{m} \right) \right).$$

We have

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

by our assumption $m \nmid h(q-1)$. We therefore obtain

$$(31) \quad \sum_{(g_1, g_2) \in \mathcal{F}^2} |a(f_1, f_2, g_1, g_2)| \leq q^{(k+2)L} - \left(\frac{\pi}{2m}\right)^2 = q^{(k+2)L} \left(1 - \frac{\pi^2}{(4m^2 q^{(k+2)L})}\right).$$

Now, we define an $|\mathcal{F}^2| \times |\mathcal{F}^2|$ matrix Z by

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

We get the inequality

$$(32) \quad \begin{aligned} & (|X(q^L I_1, \dots, q^L I_k, q^L; f_1, f_2)|)_{(f_1, f_2) \in \mathcal{F}^2} \leq \\ & \leq Z (|X(q I_1, \dots, q I_k, q; g_1, g_2)|)_{(g_1, g_2) \in \mathcal{F}^2} \end{aligned}$$

which is meant componentwise.

Let $t \in \mathbb{N}$. Due to (31), we are able to apply Lemma 3 and we obtain by the t -fold iterations of the inequality (32) together with the trivial bound

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

the inequality

$$\begin{aligned} & |X(q^{Lt} I_1, \dots, q^{Lt} I_k, q^{Lt} J; f_1, f_2)| \leq \\ & \leq \left(1 - \frac{\pi^2}{(4m^2 q^{(k+2)L})}\right)^t (q^{Lt} |I_1|) \cdots (q^{Lt} |I_k|) (q^{Lt} |J|)^2. \quad \diamond \end{aligned}$$

6. Conclusion

Let $D, B > 0$. We assume $N \geq k$. We take

$$t := \left\lfloor \frac{\log N}{8D \log \log \log N} \right\rfloor.$$

Since $d \leq (\log \log N)^D$, we have

$$L \leq \frac{\log(d(k+d))}{\log q} + 4 + k \leq 2D \left(\frac{\log \log \log N}{\log q} + 1 \right)$$

for D sufficiently large and

$$q^{Lt} \leq N^{1/4 + \log q / (4 \log \log \log N)}$$

for all $N \in \mathbb{N}$ with $(\log \log N)^D \geq k$. Thus there is an integer N_0 and some $\varepsilon > 0$, depending only on q, k and D such that for all $N \geq N_0$ we have

$$(33) \quad \frac{\sqrt{N}}{q^{Lt}} \leq N^{-\varepsilon}.$$

For any $0 < \sigma < 1$ one has $(1 - \sigma)^t < e^{-t\sigma}$. Thus we get

$$\left(1 - \frac{\pi^2}{(4m^2q^{(k+2)L})}\right)^t \ll e^{-c \log N / (\log \log \log N (\log \log N)^{(2D+1)(k+2)})},$$

where $c = \pi^2 / (36Dm^2)$. Hence

$$(34) \quad \begin{aligned} \left(1 - \frac{\pi^2}{(4m^2q^{(k+2)L})}\right)^t &\ll (\log N)^{-c \log N / (\log \log \log N (\log \log N)^{(2D+1)(k+2)+1})} \ll \\ &\ll (\log N)^{-2B}. \end{aligned}$$

Now, we are able to show (27) which yields Prop. 1 and concludes the proof of Th. 1. We need to estimate

$$X(I_1, \dots, I_k; J, f_1, f_2)$$

where the intervals satisfy (28). For $1 \leq j \leq k+1$, the integers a_j and b_j are defined by $I_j = [a_j, b_j]$ and $J = [a_{k+1}, b_{k+1}]$. Besides the integers u_j, v_j, r_j, s_j with $0 \leq r_j, s_j < q^{Lt}$ are uniquely defined by

$$a_j = q^{Lt}u_j + r_j, \quad b_j = q^{Lt}v_j + s_j$$

for all $1 \leq j \leq k+1$. Notice that $u_j \neq v_j$ by (28) and (33). We finally define

$$\tilde{I}_j := [u_j, v_j], \quad \tilde{J} := [u_{k+1}, v_{k+1}]$$

for $1 \leq j \leq k$. It is a straightforward exercise to verify

$$\begin{aligned} X(I_1, \dots, I_k, J; f_1, f_2) &= \\ &= X(q^{Lt}\tilde{I}_1, \dots, q^{Lt}\tilde{I}_k, q^{Lt}\tilde{J}; f_1, f_2) + O\left(|I_1| \cdots |I_k| |J|^2 \frac{\sqrt{N}}{q^{Lt}}\right). \end{aligned}$$

By Lemma 6, we finally get

$$X(I_1, \dots, I_k, J; f_1, f_2) \ll \left(\left(1 - \frac{\pi^2}{(4m^2q^{(k+2)L})}\right)^t + \frac{\sqrt{N}}{q^{Lt}} \right) |I_1| \cdots |I_k| |J|^2.$$

Prop. 1 is proved by applying (33) and (34).

References

- [1] BAKER, R. C. and BRÜDERN, J.: Sums of cubes of square-free numbers, *Monatsh. Math.* **111** (1991), 1–21.
- [2] BAKER, R. C. and BRÜDERN, J.: Sums of cubes of square-free numbers. II, *Monatsh. Math.* **112** (1991), 177–207.
- [3] ESTERMANN, T.: On sums of squares of square-free numbers, *Proc. London Math. Soc. (2)* **53** (1951), 125–137.
- [4] GEL/FOND, A. O.: Sur les nombres qui ont des propriétés additives et multiplicatives données, *Acta Arith.* **13** (1967/1968), 259–265.
- [5] JANCEVSKIS, M.: Convergent sieve sequences in arithmetic progressions, *J. Number Theory* **129** (2009), 1595–1607.
- [6] JANCEVSKIS, M.: A note on Waring's problem with convergent sieve sequences, *Unif. Distrib. Theory* **4** (2009).
- [7] MAUDUIT, C. and RIVAT, J.: Sur un problème de Gelfond: la somme des chiffres des nombres premiers, *Ann. Math.* **112** 177–207.
- [8] PFEIFFER, O. and THUSWALDNER, J. M.: Waring's problem restricted by a system of sum of digits congruences, *Quaest. Math.* **30** (2007), 513–523.
- [9] THUSWALDNER, J. M. and TICHY, R. F.: Waring's problem with digital restrictions, *Israel J. Math.* **149** (2005), 317–344. Probability in mathematics.
- [10] VAUGHAN, R. C.: The Hardy–Littlewood method, Cambridge Tracts in Mathematics 80, Cambridge University Press, Cambridge, 1981.
- [11] VAUGHAN, R. C.: On Waring's problem for exponents. II, *Mathematika* **33** (1986), 6–22.