TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology

DIPLOMARBEIT

# On the Nomality of Subsequences of Generalized Thue-Morse Sequences

Ausgeführt am Institut für
Diskrete Mathematik und Geometrie
der Technischen Universität Wien

unter der Anleitung von
Univ.Prof. Dipl.-Ing. Dr.techn. Michael Drmota

durch

Clemens Müllner, B.Sc.
Matrikelnummer: 0925841

Pasettistraße 72/15
1200 Wien

Datum

Unterschrift

# Preface

This diploma thesis is highly related to Gelfond's sum of digits problems, which he formulated in his paper *Sur les nombres qui ont des propriétés additives et multiplicatives données* [1] in 1968. Gelfond showed in his work that a generalized Thue-Morse sequence $\mathbf{t}_{q,m} = (s_q(n) \bmod m)_{n\in\mathbb{N}}$ is uniformly distributed along arithmetic progressions – provided that $\gcd(q, m-q) = 1$. In his work, he also formulated three more problems, which are usually called Gelfond Problems. These problems deal with uniform distribution of $\mathbf{t}_{q,m}$ along special subsequences and similar results. We cover the definitions and more details in Chapter 1.

The first problem was proven by Besineau [2] and generalized by Kim [3] in 1999. The second problem was solved by Mauduit and Rivat [4] in 2010.

We mainly consider the third problem which concerns the distribution along arbitrary integer polynomials. Mauduit and Rivat were able to solve the third problem for quadratic polynomials in 2009 [5]. Furthermore, there is a solution for prime numbers $q$ which are sufficiently large in respect to the degree of $P(x)$ by Drmota, Mauduit and Rivat [6]. The treatment of exponential sums with Fourier-theoretic methods developed by Mauduit and Rivat was a breakthrough in this field and will surely have a great impact on number theory.

The same method was used by Drmota, Mauduit and Rivat to show that $\left(\mathbf{t}_{2,2}(n^2)\right)_{n\in\mathbb{N}}$ is normal, i.e. every subsequence of length $k$ appears with asymptotic frequency $2^{-k}$.

The main goal of this thesis is to generalize this result, i.e. we show that $\left(\mathbf{t}_{q,m}(n^2)\right)_{n\in\mathbb{N}}$ is normal – provided that $\gcd(q-1, m) = 1$.

The first chapter gives some more information about the sum-of-digits function as well as Gelfond's Problems. Furthermore, an outline of the complete proof as well as a more detailed description of the following chapters are covered.

The main contribution of this work is to find appropriate bounds for Fourier terms of form

$$\mathrm{G}^I_\lambda(h,d) = \frac{1}{q^\lambda} \sum_{0\le u<q^\lambda} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell \,\mathrm{s}_\lambda(u+\ell d+i_\ell) - hq^{-\lambda}\right)$$

in this more general setting[1]. This is covered in Chapter 2.

Chapter 3 provides the necessary auxiliary results needed for Chapter 4.

Thereafter, we use the structure and ideas of [7] to deal with the occurring exponential sums. This is done in Chapter 4.

[1] We denote throughout this work the truncated sum of digits function in base $q$, i.e. the sum of the first $\lambda$ digits of $n$ in base $q$, by $s_\lambda(n)$.

## Acknowledgments

First of all, I would like to thank my supervisor, Professor Dr. Michael Drmota, who sparked my interest in number theory throughout several courses and finally drew my attention to Gelfond's Problems and, especially, the normality of $(\mathbf{t}_{q,m}(n^2))_{n\in\mathbb{N}}$. Additionally I thank him for his guidance and encouragement while working on this thesis.

I would also like to thank my colleagues and friends for supporting me throughout my studies. In particular, I would like to thank Christina Satzinger for helping me to maintain my motivation and supporting me the whole time.

Finally, I thank my family – especially my parents – for their constant support and encouragement throughout my entire life. Furthermore, I would like to thank them for arousing my interest in science.

# Contents

# 1 Introduction

At the very beginning of this thesis we want to specify the used notations:

- We denote with $\mathbb{N}, \mathbb{P}, \mathbb{Z}, \mathbb{R}$ and $\mathbb{C}$ the sets of natural numbers, prime numbers, integers, real numbers and complex numbers respectively. We additionally use $\mathbb{U}$ for the set of complex numbers with absolute value 1.
- We use the abbreviation $\log x$ for the natural logarithm of a positive real number $x$.
- We denote by $\gcd(m, n)$ the greatest common divisor of two integers $m, n$.
- As usual we denote for a real number $x$:

  $$\lfloor x \rfloor = \min\{n \in \mathbb{Z} : n \geq x\} \text{ and } ||x|| = \min\{|x - n| : n \in \mathbb{Z}\}.$$

  Furthermore, we use $x \equiv y \bmod 1$ for real numbers $x, y$ iff $x + \mathbb{Z} = y + \mathbb{Z}$.
- We write $f(x) = \mathcal{O}(g(x))$ for (real- or complex- valued) functions $f$ and $g$ if there exists a constant $C$ such that $|f(x)| \leq C|g(x)|$ for all $x$. We may alternatively write $f(x) \ll g(x)$.
- We will also use the abbreviation $\mathrm{e}(x) := \exp(2\pi i x)$ for a real number $x$.

From now on, $q$ will denote an arbitrary fixed integer $\geq 2$ throughout the entire work which will be used as the base for our expansion of natural numbers.

It is well known that any non-negative integer $n$ has a representation $n = \sum_{j \geq 0} \varepsilon_j(n) q^j$ in base $q$ where the integers $\varepsilon_j(n)$ satisfy $0 \leq \varepsilon_j(n) \leq q - 1$ and $\varepsilon_j(n) = 0$ for almost all $j \geq 0$.

The *sum of digits function* in base $q$ is defined by,

$$\mathrm{s}_q(n) := \sum_{j \geq 0} \varepsilon_j(n).$$

Since we fix $q$ at the beginning of this thesis we will use the abbreviation $\mathrm{s}(n) = \mathrm{s}_q(n)$.

## 1.1 Gelfond's Problems and their impact

We want to start this section by covering some aspects of the sum of digits function which will lead us to Gelfond's Problems. For further information on the sum of digits function see for example [8, Ch.3] or [9]. A lot of connections between automatic sequences and Gelfond's Problems as well as recent developments are covered in [10].

The sum of digits function was studied from 1850 on and arises in solutions of various problems. At the beginning of the twentieth century the Norwegian mathematician Axel Thue asked whether there is an infinite binary sequence which is *cube free*, i.e. no block of digits appears consecutively three times. He was able to show that the sequence $\mathbf{t} = (\mathrm{s}_2(n) \bmod 2)_{n \in \mathbb{N}}$ solves

this problem (see [11], [12]). This sequence has some important properties and arises in many fields.

Morse for example rediscovered this sequence in 1921 when working in differential geometry. For his work he needed to find an infinite sequence which is not periodic but every sub-sequence occurs infinitely often and with bounded gaps. Therefore, he introduced the sequence $\mathbf{t}$ independently and showed that it solves this problem (see [13] and [14]). Hence this sequence is called the **Thue-Morse sequence**.

A natural generalization of $\mathbf{t}$ is

$$\mathbf{t}_{q,m} = (\mathrm{s}_q(n) \bmod m)_{n\in\mathbb{N}}.$$

The first distributional property of $\mathbf{t}_{q,m}$ was found by Gelfond [1] who showed that – in case that $\gcd(q, m-1) = 1$ – for every $\ell \in [0, \dots, m-1]$,

$$|\{n < N : \mathrm{s}_q(an+b) \equiv \ell \bmod m\}| = \frac{N}{m} + \mathcal{O}(N^{1-\eta})$$

holds for some $\eta > 0$. However, this means exactly that linear sub-sequences of $\mathbf{t}_{q,m}$ are uniformly distributed on the values $\{0, 1, \dots, m-1\}$.

Gelfond also formulated three problems in this paper [1] which are usually called **Gelfond Problems**. All of these problems cover some more distributional properties of $\mathbf{t}_{q,m}$ and the third one is still just partly proven.

1. If $q_1, q_2 \geq 2$ are co-prime integers and $\gcd(q_1 - 1, m_1) = \gcd(q_2 - 1, m_2) = 1$ then

   $$|\{n < N : \mathrm{s}_{q_1}(n) \equiv \ell_1 \bmod m_1, \mathrm{s}_{q_2}(n) \equiv \ell_2 \bmod m_2\}| = \frac{N}{m_1 m_2} + \mathcal{O}(N^{1-\eta})$$

   for all $\ell_1, \ell_2$ and some $\eta > 0$.

2. If $q \geq 2$ and $\gcd(q-1, m) = 1$ then

   $$|\{p < N : p \in \mathbb{P} \wedge \mathrm{s}_q(p) \equiv \ell \bmod m\}| = \frac{\pi(N)}{m} + \mathcal{O}(N^{1-\eta})$$

   for all $\ell$ and some $\eta > 0$. Here $\pi(x)$ denotes the number of primes $< x$.

3. If $q \geq 2$ and $\gcd(q-1, m) = 1$ then for each integer polynomial $P(x)$

   $$|\{n < N : \mathrm{s}_q(P(n)) \equiv \ell \bmod m\}| = \frac{N}{m} + \mathcal{O}(N^{1-\eta})$$

   for all $\ell$ and some $\eta > 0$.

In 1972, Besineau was able to solve the first problem [2] and Kim was able to generalize this result to $q$-additive functions (i.e. functions which fulfill $f(aq^k + b) = f(a) + f(b)$ for $a \geq 1$, $k \geq 1, 0 \leq b < q^k$ and was also able to formulate an explicit error term [3]. However it took almost 40 years until the second and third problem were solved or came close to a solution. The second problem was solved by Mauduit and Rivat in 2010 [4]. In 2009, the third problem was also solved for quadratic polynomials by Mauduit and Rivat [5]. Additionally, there is a solution by Drmota, Mauduit and Rivat [6] for prime numbers $q$ which are sufficiently large in respect to the degree of $P(x)$. The treatment of exponential sums with Fourier-theoretic methods that

has been developed by Mauduit and Rivat was a breakthrough in this field and will also be used throughout this thesis.

We define for a sequence $(a(n))_{n\in\mathbb{N}}$ the subword complexity

$$\mathrm{p}_a(n) := |\{b_1,\dots,b_n : \exists N \in \mathbb{N} \wedge a_{N+i} = b_i \text{ for } i = 1,\dots n\}|\,.$$

It is well known that $\mathrm{p}_{\mathbf{t}_{q,m}}(n)$ is at most of linear order ($\mathcal{O}(n)$). We expect for a (quasi-) random sequence $a(n)$ with values in $\{0,\dots,m-1\}$ that $\mathrm{p}_a(n) = m^n$. Therefore, we see that the sequence $\mathbf{t}_{q,m}$ is not random at all. To introduce randomness one could take sub-sequences of the original sequence without destroying the original densities.

There have been some recent results dealing with sub-sequences along $\lfloor n^c \rfloor$ which we will not cover here. Instead we focus on the case of quadratic polynomials and especially $P(x) = x^2$. Drmota, Mauduit and Rivat recently proved that $(\mathbf{t}(n^2))_{n\in\mathbb{N}}$ is normal, i.e. every sub-sequence of length $k$ appears with asymptotic frequency $2^{-k}$ [7]. Their work has a huge impact on this thesis and we will mainly follow their ideas.

## 1.2 Outline

The goal of this thesis is to give a proof of the following theorem.

**Theorem 1.2.1.** *Let $m \in \mathbb{N}$ with $\gcd(q-1,m) = 1$. Then $(\mathbf{t}_{q,m}(n^2))_{n\in\mathbb{N}}$ is normal i.e. every sub-sequence of length $k$ appears with asymptotic frequency $q^{-k}$.*

This is obviously a generalization of the result derived by Drmota, Mauduit and Rivat in [7]. Furthermore, 1.2.1 implies that it is possible to generate non-periodic (pseudo-)random numbers modulo $m$ easily.

In order to prove our main result, we will work with exponential sums. Now we present here the main theorem on exponential sums which we will prove throughout this thesis and show its connection to Theorem 1.2.1.

From now on we also fix an arbitrary $m \in \mathbb{N}$ with $\gcd(q-1,m) = 1$.

**Theorem 1.2.2.** *For any integer $k \geq 1$ and $(\alpha_0,\dots,\alpha_{k-1}) \in \{\frac{0}{m},\dots,\frac{m-1}{m}\}^k$ such that $(\alpha_0,\dots,\alpha_{k-1}) \neq (0,\dots,0)$, there exists $\eta > 0$ such that*

$$S_0 = \sum_{n<N} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell \,\mathrm{s}((n+\ell)^2)\right) \ll N^{1-\eta}. \tag{1.1}$$

**Lemma 1.2.3.** *Theorem 1.2.2 implies Theorem 1.2.1.*

*Proof.* Let $(b_0,\dots,b_{k-1}) \in \{0,\dots,m-1\}^k$ be an arbitrary sequence of length $k$. We now count the number of occurrences of this sequence in $(\mathbf{t}_{q,m}(n^2))_{n\leq N}$. Assuming that (1.1) holds we

obtain by using the well known identity – $\sum_{n=0}^{m-1} \mathrm{e}(\frac{n}{m}\ell) = m$ for $\ell \equiv 0 \bmod m$ and 0 otherwise –

$$\begin{aligned}
&\left|\{n < N : (\mathbf{t}_{q,m}(n^2), \dots, \mathbf{t}_{q,m}((n+k-1)^2)) = (b_0, \dots, b_{k-1})\}\right| \\
&= \sum_{n<N} \mathbf{1}_{[t_{n^2}=b_0]} \cdots \mathbf{1}_{[t_{(n+k-1)^2}=b_{k-1}]} \\
&= \sum_{n<N} \prod_{\ell=0}^{k-1} \frac{1}{m} \sum_{\alpha'_\ell=0}^{m-1} \mathrm{e}\left(\frac{\alpha'_\ell}{m}\left(\mathrm{s}((n+\ell)^2) - b_\ell\right)\right) \\
&= \frac{1}{m^k} \sum_{(\alpha'_0,\dots,\alpha'_{k-1})\in\{0,\dots,p-1\}^k} \mathrm{e}\left(-\frac{\alpha'_0 b_0 + \cdots + \alpha'_{k-1} b_{k-1}}{m}\right) \sum_{n<N} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \underbrace{\frac{\alpha'_\ell}{m}}_{=:\alpha_\ell} \mathrm{s}((n+\ell)^2)\right) \\
&= \frac{N}{m^k} + \mathcal{O}\left(N^{1-\eta}\right)
\end{aligned}$$

with $\eta > 0$ obtained in Theorem 1.2.2. To obtain the last equality we separate the term with $(\alpha'_0, \dots, \alpha'_{k-1}) = 0$. □

Therefore, we concentrate on Theorem 1.2.2. The structure of the full proof of Theorem 1.2.2 is presented below.

In Chapter 2, we derive the main ingredients of the proof of Theorem 1.2.2 which are upper bounds on the Fourier terms

$$\mathrm{G}_\lambda^I(h,d) = \frac{1}{q^\lambda} \sum_{0\le u<q^\lambda} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell \,\mathrm{s}_\lambda(u+\ell d+i_\ell) - hq^{-\lambda}\right),$$

where $I = (i_0, \dots, i_{k-1}) \in \mathbb{N}^k$ with some special properties defined later.

It was necessary to introduce a new approach to find these upper bounds in our more general setting compared to [7] and we deal with them in Chapter 2. The main results of Chapter 2 are Propositions 2.2.3 and 2.2.4. Proposition 2.2.3 yields a bound on averages of Fourier transforms and the proof is similar to the proof of the corresponding result in [7]. Proposition 2.2.4 yields a uniform bound on Fourier transforms and is much harder to proof.
In Chapter 3 we derive some auxiliary results. Section 3.1 is dedicated to Vaaler's method and its application in a multidimensional setting. In Section 3.2, we prove some results on Van-der-Corput-like inequalities. These play an important role in Chapter 4 where they help us to use Fourier analytic methods. We also mention one classic result on Gauss sums in Section 3.4 as well as a short section about sums of geometric series in Section 3.3. The last Section 3.5 of this chapter treats carry propagation. This section gives a quantitative statement that carry propagation along several digits is rare.

In Chapter 4, we complete the proof for Theorem 1.2.2. We use Van-der-Corput-like inequalities in order to reduce our problem to sums depending only on few digits of $n^2, (n+1)^2, \dots, (n+k-1)^2$. We are able to reduce these quadratic terms with linear terms, which allows a proper Fourier analytic treatment. After the Fourier analysis, the remaining sum is split into two sums. The first sum involves quadratic exponential sums. The result from Section 3.4 allows us to find a proper bound here.

The Fourier terms $\mathrm{G}_\lambda^I(h,d)$ appear in the second sum and Propositions 2.2.3 and 2.2.4 will provide the necessary bounds.

For the proof of the main theorem we have to distinguish the cases $K = \alpha_0 + \cdots + \alpha_{k-1} \equiv 0 \bmod 1$ and $K \not\equiv 0 \bmod 1$. Sections 4.1 and 4.2 tackle one of these cases each. In Section 4.1, we prove that – if $K \equiv 0 \mod 1$ – we deduce Theorem 1.2.2 from Proposition 2.2.3. For $K \not\equiv 0$, Section 4.2 shows that we can deduce Theorem 1.2.2 from Proposition 2.2.4.

# 2 Generalization of Bounds on Fourier Transforms

The goal of this Chapter is to prove Propositions 2.2.3 and 2.2.4. To find the necessary bounds we first need to state one important result on the norm of matrix products. Afterwards, we deal with Fourier estimates and formulate Proposition 2.2.3 and Proposition 2.2.4. The following Sections 2.3 and 2.4 give proofs of Proposition 2.2.3 and Proposition 2.2.4 respectively.

## 2.1 Norm of matrix products

In this section we find necessary conditions under which the product of matrices decreases exponentially with respect to the matrix row-sum norm.

**Lemma 2.1.1.** *Let $\mathbf{M}_\ell$, $\ell \in \mathbb{N}$, be $N \times N$-matrices with complex entries $M_{\ell;i,j}$, for $1 \le i, j \le N$, and absolute row sums*

$$\sum_{j=1}^{N} |M_{\ell;i,j}| \le 1 \text{ for } 1 \le i \le N.$$

*Furthermore, we assume that there exist integers $m_0 \ge 1$ and $m_1 \ge 1$ and constants $c_0 > 0$ and $\eta > 0$ such that*

1. *every product $\mathbf{A} = (A_{i,j})_{(i,j)\in\{1,\dots,N\}^2}$ of $m_0$ consecutive matrices $\mathbf{M}_\ell$ has the property that,*

$$|A_{i,1}| \ge c_0 \quad \text{or} \quad \sum_{j=1}^{N} |A_{i,j}| \le 1 - \eta \text{ for every row } i; \tag{2.1}$$

2. *every product $\mathbf{B} = (B_{i,j})_{(i,j)\in\{1,\dots,N\}^2}$ of $m_1$ consecutive matrices $\mathbf{M}_\ell$ has the property*

$$\sum_{j=1}^{N} |B_{1,j}| \le 1 - \eta. \tag{2.2}$$

*Then there exist constants $C > 0$ and $\delta > 0$ such that*

$$\left\| \prod_{\ell=r}^{r+k-1} \mathbf{M}_\ell \right\|_\infty \le C q^{-\delta k} \tag{2.3}$$

*uniformly for all $r \ge 0$ and $k \ge 0$ (where $\|\cdot\|_\infty$ denotes the matrix row-sum norm).*

*Proof.* It is sufficient to show that the product of $m_0+m_1$ consecutive matrices $\mathbf{M}_\ell$ has row-sum norm $\le 1-\eta c_0$. Indeed this implies

$$\begin{aligned}\left\|\prod_{\ell=r}^{r+k-1}\mathbf{M}_\ell\right\|_\infty &\le (1-\eta c_0)^{\left\lfloor\frac{k}{m_0+m_1}\right\rfloor} \overset{(*)}{\le} \frac{1}{1-\eta c_0}\,2^{-\eta c_0\frac{k}{m_0+m_1}}\\ &\le \frac{1}{1-\eta c_0}\,q^{-\eta\frac{\log 2}{\log q}c_0\frac{k}{m_0+m_1}}\end{aligned}$$

where $(*)$ is obtained by differentiation. Thus we obtain (2.3) for $C=\frac{1}{1-\eta c_0}$ and $\delta=\eta\frac{\log 2}{\log q}\frac{c_0}{m_0+m_1}$.

Let $\mathbf{A}=(A_{i,j})_{(i,j)\in\{1,\dots,N\}^2}$ denote the product of $m_0$ consecutive matrices $\mathbf{M}_\ell$ and $\mathbf{B}=(B_{j,k})_{(j,k)\in\{1,\dots,N\}^2}$ the product of the next $m_1$ consecutive matrices $\mathbf{M}_\ell$. For any $i\in\{1,\dots,N\}$ with $|A_{i,1}|\ge c_0$, the $i$-th absolute row-sum of the product $A\cdot B$ is bounded by

$$\begin{aligned}\sum_{k=1}^N\left|\sum_{j=1}^N A_{i,j}B_{j,k}\right| &\le \sum_{j=1}^N|A_{i,j}|\sum_{k=1}^N|B_{j,k}|\\ &= |A_{i,1}|\sum_{k=1}^N|B_{1,k}|+\sum_{j=2}^N|A_{i,j}|\sum_{k=1}^N|B_{j,k}|\\ &\le |A_{i,1}|\,(1-\eta)+\sum_{j=2}^N|A_{i,j}|\\ &\le |A_{i,1}|\,(1-\eta)+1-|A_{i,1}| = 1-\eta\,|A_{i,1}|\le 1-\eta c_0.\end{aligned}$$

For $\sum_{j=1}^N|A_{i,j}|\le 1-\eta$, it holds,

$$\sum_{k=1}^N\left|\sum_{j=1}^N A_{i,j}B_{j,k}\right| \le \sum_{j=1}^N|A_{i,j}|\sum_{k=1}^N|B_{j,k}|\le 1-\eta.$$

Since $c_0\le 1$ we have $1-\eta\le 1-c_0\eta$, which completes the proof of Lemma 2.1.1. □

## 2.2 Fourier estimates

In this section, we discuss some general properties of the occurring Fourier terms. We therefore need some more definitions.

**Definition 2.2.1.** For $(\lambda,\mu)\in\mathbb{N}^2$ with $0\le\mu<\lambda$, we define the truncated $q$-ary sum-of-digits function $\mathrm{s}_\lambda$ and the two-fold restricted $q$-ary sum of digits function $\mathrm{s}_{\mu,\lambda}$ by

$$\mathrm{s}_\lambda(n)=\sum_{0\le j<\lambda}\varepsilon_j(n)\quad\text{and}\quad \mathrm{s}_{\mu,\lambda}(n)=\sum_{\mu\le j<\lambda}\varepsilon_j(n)=\mathrm{s}_\lambda(n)-\mathrm{s}_\mu(n).$$

For any $k\in\mathbb{N}$, we denote by $\mathcal{I}_k$ the set of integer vectors $I=(i_0,\dots,i_{k-1})$ with $i_0=0$ and $i_\ell\in\{i_{\ell-1},i_{\ell-1}+1\}$ for $1\le\ell\le k-1$. This set $\mathcal{I}_k$ obviously consists of $2^{k-1}$ elements. For any $I\in\mathcal{I}_k$, $h\in\mathbb{Z}$ and $(d,\lambda)\in\mathbb{N}^2$, we define,

$$\mathrm{G}_\lambda^I(h,d)=\frac{1}{q^\lambda}\sum_{0\le u<q^\lambda}\mathrm{e}\left(\sum_{\ell=0}^{k-1}\alpha_\ell\,\mathrm{s}_\lambda(u+\ell d+i_\ell)-huq^{-\lambda}\right), \tag{2.4}$$

for fixed coefficients $\alpha_\ell \in \{\frac{0}{m}, \dots, \frac{m-1}{m}\}$. This sum $G_\lambda(\,.\,, d)$ can be seen as the discrete Fourier transform of the function

$$u \mapsto \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell \, \mathrm{s}_\lambda(u + \ell d + i_\ell)\right).$$

Furthermore, we define the important parameter

$$K := \alpha_0 + \cdots + \alpha_{k-1}.$$

We start by giving a recursion for the discrete Fourier transform terms $G_\lambda^I(h,d)$ defined by (2.4). For this purpose, we define, for any $(\varepsilon, \varepsilon') \in \{0, \dots, q-1\}^2$ and $I = (i_0, i_1, \dots, i_{k-1}) \in \mathcal{I}_k$, a transformation on $\mathcal{I}_k$ by

$$\mathrm{T}_{\varepsilon\varepsilon'}(I) = \left(\left\lfloor \frac{i_\ell + \ell\varepsilon + \varepsilon'}{q} \right\rfloor\right)_{\ell \in \{0,\dots,k-1\}}.$$

If we define $f_{\varepsilon\varepsilon'}^I = \mathrm{e}\left(\sum_{l=0}^{k-1} \alpha_l \, \varepsilon_0(l\varepsilon + i_l + \varepsilon')\right)$ for $(\varepsilon, \varepsilon') \in \{0, \dots, q-1\}^2$ we immediately get the following lemma:

**Lemma 2.2.2.** *Let $I \in \mathcal{I}_k, h \in \mathbb{Z}, (d, \lambda) \in \mathbb{N}^2$ and $\varepsilon \in \{0, \dots, q-1\}$. It holds*

$$\mathrm{G}_\lambda^I(h, qd + \varepsilon) = \frac{1}{q} \sum_{\varepsilon'=0}^{q-1} f_{\varepsilon\varepsilon'}^I \, \mathrm{e}\left(-\frac{h\varepsilon'}{q^\lambda}\right) \mathrm{G}_{\lambda-1}^{T_{\varepsilon\varepsilon'}(I)}(h, d). \tag{2.5}$$

*Proof.* We evaluate $G_\lambda^I(h, qd + \varepsilon)$:

$$\begin{aligned}
\mathrm{G}_\lambda^I(h, qd+\varepsilon) &= \frac{1}{q^\lambda} \sum_{0 \le u < q^\lambda} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell \, \mathrm{s}_\lambda(u + \ell(qd+\varepsilon) + i_\ell) - huq^{-\lambda}\right) \\
&= \frac{1}{q^\lambda} \sum_{\varepsilon'=0}^{q-1} \sum_{0 \le u < q^{\lambda-1}} \mathrm{e}\left(-\frac{h(qu)}{q^\lambda}\right) \mathrm{e}\left(-\frac{h\varepsilon'}{q^\lambda}\right) \prod_{l=0}^{k-1} \mathrm{e}(\alpha_l \, \mathrm{s}_\lambda(qu + \varepsilon' + \ell(qd+\varepsilon) + i_l)) \\
&= \frac{1}{q^\lambda} \sum_{\varepsilon'=0}^{q-1} \sum_{0 \le u < q^{\lambda-1}} \mathrm{e}\left(-\frac{hu}{q^{\lambda-1}}\right) \mathrm{e}\left(-\frac{h\varepsilon'}{q^\lambda}\right) \\
&\qquad \prod_{l=0}^{k-1} \mathrm{e}\left(\alpha_l \, \mathrm{s}_{\lambda-1}\left(u + ld + \left\lfloor \frac{l\varepsilon + i_l + \varepsilon'}{q} \right\rfloor\right) + \alpha_\ell \, \varepsilon_0(l\varepsilon + i_l + \varepsilon')\right) \\
&= \frac{1}{q} \sum_{\varepsilon'=0}^{q-1} f_{\varepsilon\varepsilon'}^I \, \mathrm{e}\left(-\frac{h\varepsilon'}{q^\lambda}\right) G_{\lambda-1}^{\mathrm{T}_{\varepsilon\varepsilon'}(I)}(h, d)
\end{aligned}$$

□

As $I \in \mathcal{I}_k$ implies that $\mathrm{T}_{\varepsilon\varepsilon'}(I) \in \mathcal{I}_k$, it follows that the vector $\mathbf{G}_\lambda(h,d) = (\mathrm{G}_\lambda^I(h,d))_{I \in \mathcal{I}_k}$ can be determined recursively.

The following propositions are crucial for our proof of the main Theorem 1.2.2.

**Proposition 2.2.3.** *If $K \equiv 0 \bmod 1$ and $\frac{1}{2}\lambda \le \lambda' \le \lambda$, then there exists $\eta > 0$ such that for any $I \in \mathcal{I}_k$*

$$\frac{1}{q^{\lambda'}} \sum_{0 \le d < q^{\lambda'}} \left|\mathrm{G}_\lambda^I(h,d)\right|^2 \ll q^{-\eta\lambda}$$

*holds uniformly for all integers $h$.*

**Proposition 2.2.4.** *If $K \not\equiv 0 \bmod 1$, then there exists $\eta > 0$ such that for any $I \in \mathcal{I}_k$*

$$\left|\mathrm{G}_\lambda^I(h,d)\right| \ll q^{-\eta L} \max_{J \in \mathcal{I}_k} \left|G_{\lambda-L}^J(h, \lfloor d/q^L \rfloor)\right|$$

*holds uniformly for all non-negative integers $h, d$ and $L$.*

We give proofs for Proposition 2.2.3 and 2.2.4 in the following sections.

## 2.3 Proof of Proposition 2.2.3

This section is dedicated to the proof of Proposition 2.2.3. The idea is similar to the corresponding result in [7].

Using Lemma 2.2.2, it is easy to establish a recursion for

$$\Phi_{\lambda,\lambda'}^{I,I'}(h) = \frac{1}{q^{\lambda'}} \sum_{0 \le d < q^{\lambda'}} \mathrm{G}_\lambda^I(h,d)\overline{\mathrm{G}_\lambda^{I'}(h,d)}.$$

where $h \in \mathbb{Z}$, $(\lambda, \lambda') \in \mathbb{N}^2$ and $(I, I') \in \mathcal{I}_k^2$. For $\lambda, \lambda' \ge 1$ we have

$$\Phi_{\lambda,\lambda'}^{I,I'}(h) = \frac{1}{q^3} \sum_{\varepsilon=0}^{q-1} \sum_{\varepsilon_1=0}^{q-1} \sum_{\varepsilon_2=0}^{q-1} \mathrm{e}\left(-\frac{(\varepsilon_1-\varepsilon_2)h}{q^\lambda}\right) f_{\varepsilon\varepsilon_1}^I \overline{f_{\varepsilon\varepsilon_2}^{I'}} \Phi_{\lambda-1,\lambda'-1}^{T_{\varepsilon\varepsilon_1}(I)T_{\varepsilon\varepsilon_2}(I')}(h).$$

To find this recursion, one has to split up the sum over $0 \le d < q^{\lambda'}$ into the equivalence classes modulo $q$. This identity gives rise to a vector recursion for $\Psi_{\lambda,\lambda'}(h) = \left(\Phi_{\lambda,\lambda'}^{I,I'}(h)\right)_{(I,I') \in \mathcal{I}_k^2}$:

$$\Psi_{\lambda,\lambda'}(h) = \mathbf{M}(h/q^\lambda) \cdot \Psi_{\lambda-1,\lambda'-1}(h)$$

where the $2^{2(k-1)} \times 2^{2(k-1)}$-matrix $\mathbf{M}(\beta) = (M_{(I,I'),(J,J')}(\beta))_{((I,I'),(J,J')) \in \mathcal{I}_k^2 \times \mathcal{I}_k^2}$ is independent of $\lambda$ and $\lambda'$. By construction, all absolute row sums of $\mathbf{M}(\beta)$ are equal to 1.

It is useful to interpret these matrices as weighted directed graphs, where the vertices are the pairs $(I, I') \in \mathcal{I}_k^2$ and, starting from each vertex, there are $q^3$ directed edges to the vertices $(\mathrm{T}_{\varepsilon,\varepsilon_1}(I), \mathrm{T}_{\varepsilon,\varepsilon_2}(I'))$ (where $(\varepsilon, \varepsilon_1, \varepsilon_2) \in \{0, \dots, q-1\}^3$) with corresponding weights

$$\frac{1}{q^3} \mathrm{e}\left(-\frac{(\varepsilon_1-\varepsilon_2)h}{q^\lambda}\right) f_{\varepsilon\varepsilon_1}^I \overline{f_{\varepsilon\varepsilon_2}^{I'}}.$$

Of course, products of $m$ such matrices correspond to oriented paths of length $m$ in these graphs, which are weighted with the corresponding products. The entries at position $((I, I'), (J, J'))$ of such product matrices correspond to the sum of weights along paths from $(I, I')$ to $(J, J')$.

In order to prove Proposition 2.2.3, we will use Lemma 2.2 uniformly for $h$ with $\mathbf{M}_l = \mathbf{M}(h/q^l)$. Therefore, we need to check Conditions 2.1 and 2.2. Indeed, since $\frac{1}{2}\lambda \leq \lambda' \leq \lambda$, we have

$$\Psi_{\lambda,\lambda'}(h) = \mathbf{M}(h/q^{\lambda}) \cdots \mathbf{M}(h/q^{\lambda-\lambda'+1})\Psi_{\lambda-\lambda',0}(h).$$

**Lemma 2.3.1.** *The matrices $M_l$ defined above fulfill Condition* (2.1) *of Lemma 2.1.1.*

*Proof.* We need to show that there exists an integer $m_0 \geq 1$ such that every product

$$\mathbf{A} = (A_{(I,I'),(J,J')})_{((I,I'),(J,J')) \in \mathcal{I}_k^2 \times \mathcal{I}_k^2}$$

of $m_0$ consecutive matrices $\mathbf{M}_l = \mathbf{M}(h/q^l)$ verifies condition (1) of 2.1.1. It is obvious that $(T_{00})^{m'}(I) = \mathbf{0}$ all $I \in \mathcal{I}_k$ for sufficiently large $m'$. In the graph interpretation this means that for every vertex $(I, I')$ there is a path of length $m'$ from $(I, I')$ to $(\mathbf{0}, \mathbf{0})$. Let $m_0$ be sufficiently large and fix a row indexed by $(I, I')$ in the matrix $\mathbf{A}$. From the graph interpretation it is clear that the entry $A_{(I,I'),(\mathbf{0},\mathbf{0})}$ is the sum of at least one term of absolute value $q^{-3m_0}$. There are two possible cases. If the absolute row sum is at most

$$\leq 1 - q^{-3m_0}(2 - |1 + \mathrm{e}((q-1)\alpha_{n_0})|)/2$$

with $n_0 := \min\{n : \alpha_n \neq 0\}$, then we are done. For $\gcd(m, (q-1)) = 1$ it follows immediately that $\mathrm{e}((q-1)\alpha_{n_0}) \neq 1$ and we are bounded by $1 - \eta$ for $\eta = q^{-3m_0}(2 - |1 + \mathrm{e}((q-1)\alpha_{n_0})|)/2 > 0$.

However, if the absolute row sum is strictly greater than

$$1 - q^{-3m_0}(2 - |1 + \mathrm{e}((q-1)\alpha_{n_0})|)/2$$

it follows that $|A_{(I,I'),(\mathbf{0},\mathbf{0})}| \geq q^{-3m_0}/2$: The inequality $|A_{(I,I'),(\mathbf{0},\mathbf{0})}| < q^{-3m_0}/2$ implies that $A_{(I,I'),(\mathbf{0},\mathbf{0})}$ is the sum of at least two terms of absolute value $q^{-3m_0}$. Thus the absolute row sum would be bounded by

$$\sum_{(J,J')} |A_{(I,I'),(J,J')}| < \frac{1}{2}q^{-3m_0} + \left(1 - 2 \cdot q^{-3m_0}\right) = 1 - \frac{3}{2}q^{-3m_0} < 1 - q^{-3m_0},$$

which would contradict the assumption that the absolute row sum is strictly greater than

$$1 - q^{-3m_0}(2 - |1 + \mathrm{e}((q-1)\alpha_{n_0})|)/2 \geq 1 - q^{-3m_0}.$$

Thus we yield

$$|A_{(I,I'),(\mathbf{0},\mathbf{0})}| \geq c_0 \text{ for } c_0 = q^{-3m_0}/2.$$

□

**Lemma 2.3.2.** *The matrices $M_l$ fulfill Condition* (2.2) *of Lemma 2.1.1.*

*Proof.* Thus we need to show that there exists an integer $m_1 \geq 1$ such that for every product

$$\mathbf{B} = (B_{(I,I'),(J,J')})_{((I,I'),(J,J')) \in \mathcal{I}_k^2 \times \mathcal{I}_k^2}$$

of $m_1$ consecutive matrices $\mathbf{M}_l = \mathbf{M}(h/q^l)$ the absolute rowsum of the first row is bounded by $1 - \eta$. We concentrate on the entry $B_{(\mathbf{0},\mathbf{0}),(\mathbf{0},\mathbf{0})}$, that is, we consider all possible paths from $(\mathbf{0}, \mathbf{0})$

to $(\mathbf{0},\mathbf{0})$ of length $m_1$ in the corresponding graph and show that a positive saving for the absolute row sum is just due to the structure of this entry.

Since $T_{00}(\mathbf{0}) = T_{0(q-1)}(\mathbf{0}) = \mathbf{0}$, we have at least two paths from $(\mathbf{0},\mathbf{0})$ to $(\mathbf{0},\mathbf{0})$ and it follows that the entry $B_{(\mathbf{0},\mathbf{0}),(\mathbf{0},\mathbf{0})}$ is certainly a sum of $k_0 = k_0(m_1) \geq 2$ terms of absolute value $q^{-3m_1}$ (for every $m_1 \geq 1$). This means that there are $k_0 \geq 2$ paths from $(\mathbf{0},\mathbf{0})$ to $(\mathbf{0},\mathbf{0})$ of length $m_1$ in the corresponding graph.

We now show that we need not worry about the factors of the form $\mathrm{e}\left(-\frac{(\varepsilon_1-\varepsilon_2)h}{q^\lambda}\right)$ since we can construct a path using transformations $(T_{0\varepsilon_1}, T_{0\varepsilon_2})$ which has exactly this weight.

At first, we construct a path from $\mathbf{0}$ to $(0\ldots01\ldots1) =: I_0 \in \mathcal{I}_k$ with exactly $n_0+1$ zeroes. Therefore, let $(e_0,\ldots e_{n_1})$ be the $q$-ary representation of $n_0$, i.e. $n_0 = \sum_{j=0}^{n_1} e_j q^j$, with $n_1 = \lfloor \log_q(k-1) \rfloor$. For this section, we use the operation

$$\begin{aligned} \bar{\cdot}\colon \{0,\ldots,q-1\} &\to \{0,\ldots,q-1\} \\ x &\mapsto \overline{x} := q-1-x. \end{aligned}$$

**Claim:**

$$T_{0,\overline{e_{n_1}}} \circ T_{0,\overline{e_{n_1-1}}} \circ \ldots \circ T_{0,\overline{e_1}} \circ T_{1,\overline{e_0}}(\mathbf{0}) = I_0 \tag{2.6}$$

We define $I_{|j} = i_j$ for $I = (i_0,\ldots,i_{k-1})$ and find that $I_0$ is uniquely characterized by

$$I_{0|n_0} < I_{0|(n_0+1)},\ I_{0|(k-1)} = 1.$$

We now show this property for the left hand side of Equation (2.6). Therefore we define

$$i_{j,n} := \left(T_{0,\overline{e_n}} \circ \ldots \circ T_{1,\overline{e_0}}(I_0)\right)_{|j}.$$

**Lemma 2.3.3.** *For any $n \in \mathbb{N}$*

$$i_{n_0,n} = \left\lfloor \frac{n_0}{q^{n+1}} \right\rfloor < i_{n_0+1,n} \text{ and } i_{k-1,n} \leq 1 + \left\lfloor \frac{k-1}{q^n} \right\rfloor$$

*holds.*

*Proof.* We show this lemma by induction on $n$.

For $n=0$ we find $i_{n_0,0} = \left\lfloor \frac{n_0+q-1-e_0}{q} \right\rfloor, i_{n_0+1,0} = \left\lfloor \frac{n_0+1+q-1-e_0}{q} \right\rfloor$. Since

$$\varepsilon_0(n_0+q-1-e_0) = \varepsilon_0(e_0+q-1-e_0) = q-1$$

we conclude that $\left\lfloor \frac{n_0}{q} \right\rfloor = i_{n_0,0} < i_{n_0+1,0}$.

For $n \mapsto n+1$ we see that by applying $T_{0\overline{e_{n+1}}}$

$$i_{n_0,n+1} = \left\lfloor \frac{\left\lfloor \frac{n_0}{q^{n+1}} \right\rfloor + q - 1 - e_{n+1}}{q} \right\rfloor.$$

Since $\varepsilon_0\left(\left\lfloor\frac{n_0}{q^{n+1}}\right\rfloor+q-1-e_{n+1}\right)=\varepsilon_0(e_{n+1}+q-1-e_{n+1})=q-1$ we conclude that $\left\lfloor\frac{n_0}{q^{n+2}}\right\rfloor = i_{n_0,n+1}<i_{n_0+1,n+1}$.

Now we tackle the second part of this lemma. For $n=0$ we find $i_{k-1,0}=\left\lfloor\frac{k-1+q-1-e_0}{q}\right\rfloor\leq\left\lfloor\frac{k-1+q-1}{q}\right\rfloor\leq\left\lfloor\frac{k-1}{q}\right\rfloor+1$.
For $n\mapsto n+1$ we find that by applying $T_{0\overline{e_{n+1}}}$

$$\begin{aligned}i_{k-1,n+1}&=\left\lfloor\frac{i_{k-1,n}+q-1-e_{n+1}}{q}\right\rfloor\leq\left\lfloor\frac{1+\left\lfloor\frac{k-1}{q^{n+1}}\right\rfloor+q-1}{q}\right\rfloor=\left\lfloor1+\frac{\left\lfloor\frac{k-1}{q^{n+1}}\right\rfloor}{q}\right\rfloor\\&=1+\left\lfloor\frac{k-1}{q^{n+2}}\right\rfloor.\end{aligned}$$

□

Starting from $(\mathbf{0},\mathbf{0})$ we iteratively apply the transformations $(T_{1\overline{e_0}},T_{1\overline{e_0}}),\ldots$, and $(T_{0\overline{e_{n_1}}},T_{0\overline{e_{n_1}}})$ to reach $(I_1,I_1)$. Then we apply the transformation $(T_{00},T_{0(q-1)})$ to reach $(\mathbf{0},I_1)$ and, finally, $(T_{00},T_{00})$ to end at $(\mathbf{0},\mathbf{0})$. This corresponds to some path in the graph interpretation from $(\mathbf{0},\mathbf{0})$ to $(\mathbf{0},\mathbf{0})$ of length $m_1=n_1+4$ with weight

$$\begin{aligned}&f_{00}^{I_1}\overline{f_{0(q-1)}^{I_1}}\,\mathrm{e}\left((q-1)\frac{h}{q^{\lambda-m_1+1}}\right)\cdot\overline{f_{00}^{I_1}}q^{-3m_1}\\&\quad=\overline{f_{0(q-1)}^{I_1}}\,\mathrm{e}\left((q-1)\frac{h}{q^{\lambda-m_1+1}}\right)q^{-3m_1}\\&\quad=\mathrm{e}(-(q-1)\sum_{l=0}^{n_0}\alpha_l)\,\mathrm{e}\left((q-1)\frac{h}{q^{\lambda-m_1+1}}\right)q^{-3m_1}\\&\quad=\mathrm{e}(-(q-1)\alpha_{n_0})\,\mathrm{e}\left((q-1)\frac{h}{q^{\lambda-m_1+1}}\right)q^{-3m_1}.\end{aligned}$$

Next, we construct some path with weight $\mathrm{e}((q-1)h/q^{\lambda-m_1+1})q^{-3m_1}$. Starting from $(\mathbf{0},\mathbf{0})$ we first apply $m_1-2$ times the transformations $(T_{00},T_{00})$, then one time the transformation $(T_{00},T_{0(q-1)})$, and then one time the transformation $(T_{00},T_{00})$. This corresponds in the graph interpretation to a path from $(\mathbf{0},\mathbf{0})$ to $(\mathbf{0},\mathbf{0})$ of length $m_1$ with weight

$$\begin{aligned}\mathrm{e}\left(\sum_{l=0}^{k-1}\alpha_l(q-1)\right)\cdot\mathrm{e}\left((q-1)\frac{h}{q^{\lambda-m_1+1}}\right)q^{-3m_1}&=\mathrm{e}(K(q-1))\cdot\mathrm{e}\left((q-1)\frac{h}{q^{\lambda-m_1+1}}\right)q^{-3m_1}\\&=\mathrm{e}\left((q-1)\frac{h}{q^{\lambda-m_1+1}}\right)q^{-3m_1}.\end{aligned}$$

We finally see that

$$\begin{aligned}|B_{(\mathbf{0},\mathbf{0}),(\mathbf{0},\mathbf{0})}|&\leq\left(k_0-2+\left|\mathrm{e}\left((q-1)\frac{h}{q^{\lambda-m_1+1}}\right)+\mathrm{e}\left((q-1)\frac{h}{q^{\lambda-m_1+1}}\right)\mathrm{e}(-(q-1)\alpha_{n_0})\right|\right)q^{-3m_1}\\&=(k_0-2+|1+\mathrm{e}((q-1)\alpha_{n_0})|)q^{-3m_1},\end{aligned}$$

so that

$$\sum_{(J,J')} |B_{(0,0),(J,J')}| \le (k_0 - 2 + |1 + \mathrm{e}((q-1)\alpha_{n_0})|)q^{-3m_1} + (1 - k_0 q^{-3m_1})$$
$$\le 1 - (2 - |1 + \mathrm{e}((q-1)\alpha_{n_0})|) \cdot q^{-3m_1}.$$

Therefore condition (2.2) of Lemma 2.1.1 is verified with $\eta = (2 - |1 + \mathrm{e}((q-1)\alpha_{n_0})|) \cdot q^{-3m_1}$. □

At the end of this section we want to recall the important steps of the proof of Proposition 2.2.3. At first we find that

$$\frac{1}{q^{\lambda'}} \sum_{0 \le d < q^{\lambda'}} |G_\lambda^I(h,d)|^2 = \Phi_{\lambda,\lambda'}^{I,I}(h).$$

Thus Proposition 2.2.3 is equivalent to $\Phi_{\lambda,\lambda'}^{I,I}(h) \ll q^{-\eta\lambda}$. Next we considered the vector $\Psi_{\lambda,\lambda'}(h) = \left(\Phi_{\lambda,\lambda'}^{I,I'}(h)\right)_{(I,I') \in \mathcal{I}_k^2}$ and found the recursion

$$\Psi_{\lambda,\lambda'}(h) = M(h/q^\lambda) \cdots M(h/q^{\lambda-\lambda'+1}) \Psi_{\lambda-\lambda',0}(h)$$

Then we defined $M_\ell := M(h/q^\ell)$ and showed that we can apply Lemma 2.1.1. Therefore we know that – since $\left|\Phi_{\lambda-\lambda'+1,0}^{I,I'}(h)\right| \le 1$

$$|\Phi_{\lambda,\lambda'}^{I,I'}(h)| \le \|M_\lambda \cdots M_{\lambda-\lambda'+1}\|_\infty \le C q^{-\delta\lambda'} \le C q^{-\delta\lambda/2}$$

with $C$ and $\delta$ obtained by Lemma 2.1.1. Thus we know that $\Phi_{\lambda,\lambda'}^{I,I'}(h) \ll q^{-\eta\lambda}$ with $\eta = \delta/2$ uniformly for all $h$.

## 2.4 Proof of Proposition 2.2.4

This section deals with the proof of Proposition 2.2.4. Compared to [7] we follow a completely new idea. We have to take many sequences $\mathbf{e}$ into account whereas in [7] it was sufficient to find one specific sequence.

We start by formulating Equation (2.5) as a matrix vector multiplication:

$$G_\lambda(h,d) = \frac{1}{q} M^{\varepsilon_0(d)}\left(\mathrm{e}\left(-\frac{h}{q^\lambda}\right)\right) G_{\lambda-1}\left(h, \left\lfloor \frac{d}{q} \right\rfloor\right)$$

where for any $\varepsilon \in \{0, \dots, q-1\}$ and $z \in \mathbb{U}$ we have

$$M^\varepsilon(z) = \sum_{\varepsilon'=0}^{q-1} (\mathbf{1}_{[J = T_{\varepsilon\varepsilon'}(I)]} f_{\varepsilon\varepsilon'}^I z^{\varepsilon'})_{(I,J) \in \mathcal{I}_k^2}.$$

When iteratively applying this formula, we yield for $m' \ge 1$,

$$G_\lambda(h,d) = \frac{1}{q^{m'}} M^{(\varepsilon_0(d), \dots, \varepsilon_{m'-1}(d))}\left(\mathrm{e}\left(-\frac{h}{q^\lambda}\right)\right) G_{\lambda-m'}\left(h, \left\lfloor \frac{d}{q^{m'}} \right\rfloor\right),$$

where, for any $\mathbf{d} = (d_0, \dots, d_{m'-1}) \in \{0,1\}^{m'}$, $M^{\mathbf{d}}(z)$ denotes the product of the corresponding matrices, i.e.

$$M^{\mathbf{d}}(z) = M^{d_0}(z) \cdot M^{d_1}(z^q) \cdots M^{d_{m'-1}}(z^{q^{m'-1}}).$$

The matrix elements $P_{IJ}^{\mathbf{d}}, (I,J) \in \mathcal{I}_k^2$ with

$$M^{\mathbf{d}}(z) = (P_{IJ}^{\mathbf{d}}(z))_{(I,J)\in\mathcal{I}_k^2},$$

are polynomials in $z$ and

$$\left\| M^{\mathbf{d}}(z) \right\|_\infty = \max_{I\in\mathcal{I}_k} \max_{z\in\mathbb{U}} \sum_{J\in\mathcal{I}_k} |P_{IJ}^{\mathbf{d}}(z)|$$

holds.

Using Lemma 2.1.1, Proposition 2.2.4 follows from the fact that there exists an integer $m' \geq 1$ such that for any $\mathbf{d} \in \{0,\dots,q-1\}^{m'}$ and $I \in \mathcal{I}_k$,

$$\max_{z\in\mathbb{U}} \sum_{J\in\mathcal{I}_k} |P_{IJ}^{\mathbf{d}}(z)| < q^{m'}, \tag{2.7}$$

i.e. the trivial bound $q^{m'}$ is not sharp.

*Example.* Consider the case $q = 3, I = (0,\dots,0), \mathbf{d} = (0,0)$. We want to compute $P_{IJ}^{\mathbf{d}}(z)$.

Obviously $T_{0\varepsilon}(I) = I$ holds for $\varepsilon \in \{0,1,2\}$. Therefore, we know that $P_{IJ}^{\mathbf{d}}(z) = 0$ for any $J \neq I$. It is easy to see that $f_{0\varepsilon}^I = \mathrm{e}(K\varepsilon)$. Therefore we find

$$P_{II}^{\mathbf{d}}(z) = (1 + z\,\mathrm{e}(K) + z^2\,\mathrm{e}(2K)) \cdot (1 + z^3\,\mathrm{e}(K) + z^6\,\mathrm{e}(2K)).$$

We want to show that the strict inequality 2.7 holds and find that

$$\max_{z\in\mathbb{U}} \sum_{J\in\mathcal{I}_k} |P_{IJ}^{\mathbf{d}}(z)| = \max_{z\in\mathbb{U}} |1 + z\,\mathrm{e}(K) + z^2\,\mathrm{e}(2K)| \cdot |1 + z^3\,\mathrm{e}(K) + z^6\,\mathrm{e}(2K)|.$$

We see that $|1 + z^\ell\,\mathrm{e}(K) + z^{2\ell}\,\mathrm{e}(2K)| \leq |1 + z^\ell\,\mathrm{e}(K)| + |z^{2\ell}\,\mathrm{e}(2K)| \leq 3$ (with $\ell = 1,3$) and for equality to hold it is necessary that $z^\ell = \mathrm{e}(-K)$. Therefore $\mathrm{e}(-3K) = z^3 = \mathrm{e}(-K)$ which can only hold for $2K \equiv 0 \bmod 1$. Since $mK \in \mathbb{Z}$, this is equivlaent to $2mK \equiv 0 \bmod m$ and by $\gcd(q-1,m) = 1$ it follows that $mK \equiv 0 \bmod m$ and, therefore, $K \equiv 0 \bmod 1$ which yields a contradiction. This example provides some crucial aspects for the proof of Proposition 2.2.4.

For $\mathbf{d} = (d_0,\dots,d_{m'-1}) \in \{0,\dots,q-1\}^{m'}$, we interpret the coefficients of the matrix $M^{\mathbf{d}}(z)$ as encoding of paths of length $m'$.

For $I \in \mathcal{I}_k, \mathbf{e} = (e_0,\dots,e_{j-1}) \in \{0,\dots,q-1\}^j$ and $i \in \{1,\dots,\max\{m',j\}\}$, we define

$$T_i^{\mathbf{de}}(I) = T_{d_{i-1}e_{i-1}} \circ \cdots \circ T_{d_0e_0}(I)$$

and associate to each of the $q^{m'}$ paths from the vertex $I$ to the vertices $T_{m'}^{\mathbf{de}}(I)$ the weight

$$w^{\mathbf{de}}(I,z) = f_{d_0e_0}^I z^{e_0} f_{d_1e_1}^{T_1^{\mathbf{de}}(I)} z^{q^1e_1} \cdots f_{d_{m'-1}e_{m'-1}}^{T_{m'-1}^{\mathbf{de}}(I)} z^{q^{m'-1}e_{m'-1}}.$$

Therefore $w^{\mathbf{de}}(I,z) = v(I,\mathbf{d},\mathbf{e})z^{N(e)}$ holds with

$$v(I,\mathbf{d},\mathbf{e}) = f^{I}_{d_0e_0} \cdot f^{T_1^{\mathbf{de}}(I)}_{d_1e_1} \cdots f^{T^{\mathbf{de}}_{m'-1}(I)}_{d_{m'-1}e_{m'-1}} \text{ and } N(\mathbf{e}) = \sum_{i=0}^{m'-1} e_i q^i.$$

We need another short lemma:

**Lemma 2.4.1.** *Let $(I_0,I_1) \in \mathcal{I}_k^2$ and $j \in \{0,\ldots,k-1\}$ such that $I_{1|j} - I_{0|j} = 1$ and $\varepsilon \in \{0,\ldots,q-1\}$. Then there exists exactly one $\varepsilon \in \{0,\ldots,q-1\}$ such that*

$$T_{\varepsilon\varepsilon'}(I_0)_{|j} + 1 = T_{\varepsilon\varepsilon'}(I_1)_{|j}$$

*and for $\varepsilon'' \neq \varepsilon$*

$$T_{\varepsilon''\varepsilon'}(I_0)_{|j} = T_{\varepsilon''\varepsilon'}(I_1)_{|j}.$$

*Proof.* We see by definition that $T_{\varepsilon\varepsilon'}(I)_{|j} = \left\lfloor \frac{I_{|j}+j\varepsilon+\varepsilon'}{q} \right\rfloor$. Therefore, Lemma 2.4.1 follows easily from the fact that $T_{\varepsilon\varepsilon'}(I_0)_{|j} + 1 = T_{\varepsilon\varepsilon'}(I_1)_{|j}$ holds iff $I_{1|j} + j\varepsilon + \varepsilon' \equiv 0 \mod q$. □

We denote by $(\varepsilon \circ \mathbf{f}) = (\varepsilon, f_0, \ldots, f_n)$ for $\mathbf{f} = (f_0,\ldots,f_n)$ the usual concatenation.

We, furthermore, fix a vector $\mathbf{d} = (d_0,\ldots,d_{m'-1}) \in \{0,\ldots,q-1\}^{m'}$ and a $\delta \in \{0,\ldots,q-1\}$ and define

$$\begin{aligned}
&\mathbf{d}' := (\delta \circ \mathbf{d})\\
&I_\varepsilon := T_{\varepsilon\delta}(I)\\
&M := \{j \in \{0,\ldots,k-1\} : I_{0|j} \neq I_{1|j}\}.
\end{aligned}$$

It is easy to see that $T_{1|j} = T_{0|j} + 1$ for any $j \in M$.

We are now interested in paths starting at $I_0$, $I_1$ and meet along their ways $T^{\mathbf{de}}_{m'}(\,.\,)$ and end at the same $J \in \mathcal{I}_k$ – obviously they do not part again in any position. We say **e corrects a position** $j \in M$ **at step** $k \geq 0$ if $k$ is the minimal integer such that $T^{\mathbf{de}}_k(I_0)_{|j} = T^{\mathbf{de}}_k(I_1)_{|j}$. We say **e corrects a position** $j \in M$ if there exists $k$ such that $\mathbf{e}$ corrects $j$ at step $k$.

**Lemma 2.4.2.** *For any sequence $\mathbf{e} \in \{0,\ldots,q-1\}^{m'}$ that corrects all positions,*

$$v(\mathbf{e}) := v(I,\mathbf{d}',(0\circ\mathbf{e}))v(I,\mathbf{d}',(1\circ\mathbf{e}))^{-1} = \mathrm{e}(-K)\prod_{j\in M}\mathrm{e}(\alpha_j(q-1)k_j))$$

*holds, where $k_j = k_j(\mathbf{e})$ denotes the step at which position $j$ is corrected and depends on $\mathbf{e}$.*

*Proof.* By the multiplicative structure of $v(I,\mathbf{d}',\mathbf{e}')$, we can compute $v(\mathbf{e})$ for each position $j \in \{0,\ldots,k-1\}$ independently:

For $j \notin M$, $T_{\delta 0}(I)_{|j} = T_{\delta 1}(I)_{|j}$ holds and, therefore, we know that $\varepsilon_0(i_j + j\delta + 1) = l \in \{1,\ldots,q-1\}$. Thus we get a factor $\mathrm{e}((l-1)\alpha_j)\,\mathrm{e}(-l\alpha_j) = \mathrm{e}(-\alpha_j)$ for $v(\mathbf{e})$ resulting from the first step.

For the subsequent steps we know that $T_i^{\mathbf{d}'(0\circ\mathbf{e})}(I)_{|j} = T_i^{\mathbf{d}'(1\circ\mathbf{e})}(I)_{|j}$ and, therefore, the two factors always cancel each other out.

For $j \in M$, we know that $T^{\delta 0}(I)_{|j} + 1 = T^{\delta 1}(I)_{|j}$ and, therefore, $\varepsilon_0(i_j + j\delta + 1) = 0$ and thus we receive a factor $\mathrm{e}((q-1)\alpha_j)$ for the first step.

By definition, position $j$ is corrected at step $k_j$ and thus for $i < k_j$

$$T_i^{\mathbf{d}'(0\circ\mathbf{e})}(I)_{|j} + 1 = T_i^{\mathbf{d}'(1\circ\mathbf{e})}(I)_{|j}.$$

Therefore we yield

$$\varepsilon_0\left(T_{i-1}^{\mathbf{d}'(0\circ\mathbf{e})}(I)_{|j} + jd_{i-1} + e_{i-1}\right) = q-1 \text{ and } \varepsilon_0\left(T_{i-1}^{\mathbf{d}'(1\circ\mathbf{e})}(I)_{|j} + jd_{i-1} + e_{i-1}\right) = 0$$

and we receive a factor $\mathrm{e}((q-1)\alpha_j)$ for every step $i < k_j$.

For $i = k_j$ we know that

$$\varepsilon_0(T_{i-1}^{\mathbf{d}'(1\circ\mathbf{e})}(I)_{|j} + jd_{i-1} + e_{i-1}) = l \in \{1, \dots, q-1\} \text{ and } \varepsilon_0(T_{i-1}^{\mathbf{d}'(0\circ\mathbf{e})}(I)_{|j} + jd_{i-1} + e_{i-1}) = l - 1.$$

Therefore we get a factor $\mathrm{e}(-\alpha_j)$.

As for $j \notin M$, we do not get any contribution for $i > k_j$.

Altogether we find $v(I, \mathbf{d}', (0\circ\mathbf{e}))v(I, \mathbf{d}', (1\circ\mathbf{e}))^{-1} = \prod_{j\notin M} \mathrm{e}(-\alpha_j) \prod_{j\in M} \mathrm{e}(\alpha_j((q-1)k_j - 1))$. □

For any sequence $\mathbf{e} \in \{0, \dots, q-1\}^{m'}$, correcting all positions is equivalent to

$$J := T_{m'}^{\mathbf{d}'(0\circ\mathbf{e})}(I) = T_{m'}^{\mathbf{d}'(1\circ\mathbf{e})}(I).$$

Therefore, we know by $N(1\circ\mathbf{e}) = N(0\circ\mathbf{e}) + 1$

$$|z^{N(0\circ\mathbf{e})}v(I, \mathbf{d}', (0\circ\mathbf{e})) + z^{N(1\circ\mathbf{e})}v(I, \mathbf{d}', (1\circ\mathbf{e}))| = |v(\mathbf{e}) + z| \le 2.$$

Equality obviously just holds for $z = v(\mathbf{e})$ where $v(\mathbf{e})$ only depends on the values of $k_j(\mathbf{e})$. Since $(0\circ\mathbf{e})$ and $(1\circ\mathbf{e})$ encode paths from $I$ to $J$, the summand mentioned above occurs in $P_{IJ}^{\mathbf{d}}(z)$ and, by applying the triangle inequality, equality in (2.7) can only hold for $z = v(\mathbf{e})$.

The rest of this proof is devoted to finding pairs of sequences $(\mathbf{e}, \mathbf{e}')$ such that the values of the corresponding $k_j$ do not "'differ a lot"'. This gives rise to restrictions of the values $\alpha_j$ and leads to a restriction for the value $z$ for which equality in Inequality (2.7) can hold. To complete the proof, we use the fact that the row sum norm is submultiplicative to contradict the assumption $K \not\equiv 0 \bmod 1$ provided that equality holds for (2.7).

*Example.* Let $I = (0, \dots, 0), \mathbf{d}' = (0, \dots, 0)$. We want to compute $\nu(\mathbf{e})$ "'by hand"' for all sequences $\mathbf{e}$. It is easy to see that $I_0 = I_1 = I$ (i.e. the paths never differ) and $f_{00}^I = 1, f_{01}^I = \mathrm{e}(K)$. Therefore, we find $\nu(\mathbf{e}) = \mathrm{e}(-K)$ for any sequence $\mathbf{e}$.

We can also use Lemma 2.4.2 to compute $\nu(\mathbf{e})$. We just need to see that $M = \emptyset$ and thus $\nu(\mathbf{e}) = \prod_j \mathrm{e}(-\alpha_j) = \mathrm{e}(-K)$.

As we observed in the example above, one possible value of $z$ for which equality in (2.7) can hold is $\mathrm{e}(-K)$. The factor $\mathrm{e}(-K)$ appears in $v(\mathbf{e})$ and we want to show that equality can just hold for $z = \mathrm{e}(-K)$ for arbitrary $\mathbf{d}'$ and $I$. It would be sufficient to find for all $j' \in M$ sequences $\mathbf{e}, \mathbf{e}'$

such that the values of $k_j(\mathbf{e})$, $k_j(\mathbf{e}')$ coincide for all $j$ except $j'$, where they differ by one. For equality to hold we would need that $z = v(\mathbf{e}) = v(\mathbf{e}')$ and, therefore, the quotient

$$\frac{v(\mathrm{e})}{v(\mathrm{e}')} = \mathrm{e}((q-1)\alpha_{j'}) = 1.$$

Therefore, we would conclude $v(\mathbf{e}) = \mathrm{e}(-K)$ for any $\mathbf{e}$ that corrects all positions.

Unfortunately, there might be positions $j$, $j'$ that always get corrected at the same step for each sequence $\mathbf{e}$ – even for large values of $m'$. Therefore, changing the value of $k_j$ also changes the value of $k_{j'}$.

*Example.* Let $\mathbf{d}' = (0,\ldots,0), I = (0,1,2,\ldots,q-2,q-1,q-1,q-1)$. A quick computation yields $I_0 = (0,\ldots,0), I_1 = (0,\ldots,0,1,1,1)$, and $M = \{q-1,q,q+1\}$.

Since $T^{00}(I_1) = \ldots = T^{0(q-2)}(I_1) = (0,\ldots,0)$ and $T^{0(q-1)}(I_1) = I_1$, we see that position $q-1$ is corrected at step $k$ iff $\mathbf{e}$ is of form $(q-1,\ldots,q-1,x,\ldots)$ where $0 \le x < q-1$. This sequence also corrects positions $q$ and $q+1$ at step $k$ and, therefore, positions $q-1, q, q+1$ are corrected at the same step for each sequence $\mathbf{e}$.

To deal with the problem stated above, we define $M(\mathbf{e},n)$ to be the positions which are not corrected by e after $n$ steps and with this notation we define

**Definition 2.4.3** (admissible starting-sequence)**.** $\mathbf{e} \in \{0,\ldots,q-1\}^l$ is called an **admissible starting-sequence** of length $l$ iff for $n \le l-2$ it holds that $M(\mathbf{e},n) \neq M(\mathbf{e},n+2)$ or $M(\mathbf{e},n) = \emptyset$.

**Definition 2.4.4** (admissible sequence)**.** An admissible starting-sequence of length $m'$ is called an **admissible sequence**.

If $m' \ge 2(k-1)$, it is easy to see that any position will be corrected by an admissible sequence and we will assume from now on that $m' \ge 2(k-1)$, if not stated otherwise.

**Lemma 2.4.5.** *Every admissible starting-sequence* $\mathbf{e}$ *of length* $l \le m'$ *can be extended to an admissible sequence* $\mathbf{e}' = (e_0,\ldots,e_{l-1},e_l,\ldots,e_{m-1})$.

*Proof.* We define $e_j$ for $j > l$ recursively: Let $i_j$ be the minimal index for which $T_j^{\mathbf{de}}(I_0)_{|i_j} + 1 = T_j^{\mathbf{de}}(I_1)_{|i_j}$. By Lemma 2.4.1, we know that $e_j = 0$ or $e_j = 1$ implies that $\mathbf{e}$ corrects position $i_j$ at step $j$. If there is no such index $i_j$, we define $e_j$ arbitrarily. □

**Lemma 2.4.6.** *For any* $j \in M$ *and for any integer* $0 \le l \le m'$*, there exists exactly one* $\mathbf{e} \in \{0,\ldots,q-1\}^l$ *such that* $T_l^{\mathbf{de}}(I_0)_{|j} + 1 = T_l^{\mathbf{de}}(I_1)_{|j}$.

*Proof.* This results follows by induction on $l$:
Let $\mathbf{e} = (e_0,\ldots,e_{l-1})$ and $T_l^{\mathbf{de}}(I_0)_{|j} + 1 = T_l^{\mathbf{de}}(I_1)_{|j}$. By Lemma 2.4.1, position $j$ is corrected at step $l+1$ for exactly one $e_l = \varepsilon' \in \{0,\ldots,q-1\}$. □

It follows easily that for each subset $M' \subseteq M$ there is at most one (admissible starting) sequence of length $l$ that does not correct $M'$.

We now define a relation $\sim$ on $M$ as follows:

$$i \sim j \Leftrightarrow \text{each admissible sequence } \mathbf{e} \text{ corrects } i \text{ at step } k \text{ iff it corrects } j \text{ at step } k.$$

Obviously $\sim$ is an equivalence relation and corresponds to a partition $\mathcal{P} = \{P_1, \dots, P_n\}$ of $M$.

If $\mathbf{e}$ is an admissible sequence and $1 \leq j \leq n$, then all $i \in P_j$ are corrected at the same step by $\mathbf{e}$, which we define as $n_j(\mathbf{e})$. By definition, $k_i(\mathrm{e}) = n_j(\mathrm{e}), \forall i \in P_j$.

Instead of finding pairs of sequences $\mathbf{e}$, $\mathbf{e}'$ for all $j' \in M$ such that the values of $k_j(\mathrm{e})$, $k_j(\mathrm{e}')$ coincide for all $j$ except $j'$, we combine the positions according to $\sim$. We want to motivate this by the following example:

*Example.* Let $q = 3$, $I = (0,0,0,1,1,2,3,4)$, $\mathbf{d}' = (1,1,1,1)$. We find

$$I_0 = (0,0,0,1,1,2,3,3), I_1 = (0,0,1,1,2,2,3,4)$$

and, therefore, $M = \{2,4,7\}$. We compute

$$T^{10}(I_0) = (0,0,0,1,1,2,3,3),\ T^{10}(I_1) = (0,0,1,1,2,2,3,3)$$
$$T^{11}(I_0) = (0,0,1,1,2,2,3,3),\ T^{11}(I_1) = (0,0,1,1,2,2,3,4).$$

Consequently $M((0,0,0),1) = \{2,4\}$ and $M((1,1,1),1) = \{7\}$. As $(0,0,0,1,1,2,3,3)$, $(0,0,1,1,2,2,3,3)$ are fixed points of $T^{10}$ and $(0,0,1,1,2,2,3,3)$, $(0,0,1,1,2,2,3,4)$ are fixed points of $T^{11}$, we see that $\mathcal{P} = \{\{2,4\},\{7\}\}$.

We find the following sequences

$$\mathbf{e}_1 = (0,0,1) \text{ with } n_1(\mathbf{e}_1) = 3,\ n_2(\mathbf{e}_1) = 1$$
$$\mathbf{e}_1' = (0,1,0) \text{ with } n_1(\mathbf{e}_1') = 2,\ n_2(\mathbf{e}_1') = 1$$
$$\mathbf{e}_2 = (1,1,0) \text{ with } n_1(\mathbf{e}_2) = 1,\ n_2(\mathbf{e}_2) = 3$$
$$\mathbf{e}_2' = (1,0,2) \text{ with } n_1(\mathbf{e}_2') = 1,\ n_2(\mathbf{e}_2') = 2.$$

So we found pairs of sequences for which their values of $n_j$ coincide or differ by one once. We want to prove that it is always possible to find such sequences:

**Lemma 2.4.7.** *For any $1 \leq j \leq n$, there are two admissible sequences $\mathbf{e}, \mathbf{e}'$ such that $n_i(\mathbf{e}) = n_i(\mathbf{e}')$ for any $i \neq j$ and $n_j(\mathbf{e}) + 1 = n_j(\mathbf{e}')$.*

*Proof.* For this proof, we denote with $\overline{\varepsilon}$ an arbitrary integer with $0 \leq \overline{\varepsilon} \leq q-1$ and $\overline{\varepsilon} \neq \varepsilon$. Let $\mathbf{e}' = (e_0, \dots, e_{m'-1})$ be an admissible sequence which maximizes $n_j(\mathrm{e}')$.

Since any position is corrected by $\mathbf{e}'$ and $n_j(\mathbf{e}')$ is maximal we show that $n_j(\mathbf{e}') \geq n_{j'}(\mathbf{e}')$ for all $j' \leq n$: If $n_{j'}(\mathrm{e}') > n_j(\mathrm{e}')$ we could find an admissible starting sequence $\mathbf{e}^* = (e_0, \dots, e_{n_j(\mathbf{e}')-1}, \overline{e_{n_j(\mathbf{e}')}})$. $\mathbf{e}^*$ does not correct $P_j$ and corrects at least $P_{j'}$ at the last step and is therefore extendable to an admissible sequence $\mathbf{f}$ with $n_j(\mathbf{f}) > n_j(\mathbf{e}')$ which yields a contradiction to the maximality of $n_j(\mathrm{e}')$.

Next, we observe that no position is corrected by $\mathbf{e}'$ at step $n_j(\mathbf{e}') - 1$; otherwise $\mathbf{e}^* = (e_0, \dots, e_{n_j(\mathbf{e}')-1}, \overline{e_{n_j(\mathbf{e}')}})$ would again be an admissible starting sequence and would be extendable to an admissible sequence $\mathbf{f}$ with $n_j(\mathbf{f}) > n_j(\mathbf{e}')$.

Therefore, we know that $\mathbf{e} = (e_0, \dots, e_{n_j(\mathbf{e}')-2}, \overline{e_{n_j(\mathbf{e}')-1}}, 0, \dots, 0)$ is an admissible sequence with $n_j(\mathbf{e}) + 1 = n_j(\mathbf{e}')$.

It remains to show that $n_i(\mathbf{e}) = n_i(\mathbf{e}')$ for all $i \neq j$; assume that $n_i(\mathbf{e}) \neq n_i(\mathbf{e}')$. We note that $n_i(\mathbf{e}') \leq n_j(\mathbf{e}')$ and $n_i(\mathbf{e}') \neq n_j(\mathrm{e}') - 1$ by the arguments above. Furthermore, $n_i(\mathrm{e}') \leq$

$n_j(\mathrm{e}') - 2$ would imply that $n_i(\mathrm{e}) = n_i(\mathrm{e}')$. Therefore, it remains to consider the case $n_i(\mathrm{e}') = n_j(\mathrm{e}')$. By Lemma 2.4.6, we know that any admissible starting-sequence of length $n_0 < n_j(\mathbf{e}')$ which does correct $P_j$ at step $n_0$ is of form $(e_0, \ldots, e_{n_0-1}, \overline{e_{n_0}})$. By Lemma 2.4.1, we know that $(e_0, \ldots, e_{n_0-1}, \overline{e_{n_0}})$ also corrects $P_i$ at step $n_0$. Since any admissible sequence $\mathbf{f}$ corrects $P_j$ at step $n_j(\mathbf{f}) \leq n_j(\mathbf{e}')$ we know that it also corrects $P_i$ at step $n_j(\mathbf{f})$ and, therefore, $P_i \sim P_j$ which yields a contradiction. □

This proof also shows that $\mathbf{e}, \mathbf{e}'$ are distinct for all $j$.

We define $\beta_j = \sum_{l \in P_j} \alpha_l$ and immediately obtain the following corollary.

**Corollary 2.4.8.** *For any admissible sequence* $\mathbf{e}$

$$v(I, \mathbf{d}', (0 \circ \mathbf{e}))v(I, \mathbf{d}', (1 \circ \mathbf{e}))^{-1} = \mathrm{e}(-K) \prod_{j=1}^{l} \mathrm{e}((q-1)\beta_j n_j) \tag{2.8}$$

*holds, where* $n_j = n_j(\mathbf{e})$.

*Proof.* This is an immediate consequence of Lemma 2.4.2. □

We are now prepared to show the following lemma.

**Lemma 2.4.9.** *For* $z \in \mathbb{U}$ *and* $m' \geq 2k - 1$

$$\sum_{J \in \mathcal{I}_k} |P_{IJ}^{\mathbf{d}'}(z)| = q^{m'} \tag{2.9}$$

*holds at most for* $z = \mathrm{e}(-K)$.

*Proof.* At first we want to show that, if there exists a $z \in \mathbb{U}$ such that (2.9) holds, it follows that $(q-1)\beta_j \equiv 0 \mod 1$ for $j = 1, \ldots, n$:
By Lemma 2.4.7, we know that there exist, for any $1 \leq j \leq n$, admissible sequences $\mathbf{e}, \mathbf{e}'$ such that $n_j(\mathbf{e}') = n_j(\mathbf{e}) + 1$ and for any $i \neq j : n_i(\mathbf{e}') = n_i(\mathbf{e})$. We already observed that for any admissible sequence $\mathbf{f}$, $T^{\mathbf{d}'(0 \circ \mathbf{f})}(I) = T^{\mathbf{d}'(1 \circ \mathbf{f})}(I)$ holds. We see that

$$|P_{IJ}^{\mathbf{d}'}(z)| = |\ldots + v(I, \mathbf{d}', (0 \circ \mathbf{f}))z^{0+qN(\mathbf{f})} + v(I, \mathbf{d}', (1 \circ \mathbf{f}))z^{1+qN(\mathbf{f})} + \ldots|.$$

By applying the triangle inequality we can isolate the term:

$$\underbrace{|v(I, \mathbf{d}', (1 \circ \mathbf{f}))z^{qN(\mathbf{f})}|}_{=1} \cdot |v(\mathbf{f}) + z|.$$

For equality to hold at Equation (2.9) there has to hold $z = v(\mathbf{f})$. Using this fact for $\mathbf{e}, \mathbf{e}'$ obtained by Lemma 2.4.7 we yield

$$z = v(\mathbf{e}) = \mathrm{e}(-K) \prod_{i=1}^{l} \mathrm{e}((q-1)n_i(\mathbf{e})\beta_i)$$

$$z = v(\mathbf{e}') = \mathrm{e}(-K) \prod_{i=1}^{l} \mathrm{e}((q-1)n_i(\mathbf{e}')\beta_i)$$

and therefore

$$\begin{aligned} 1 &= \prod_{i=1}^{l} \mathrm{e}((q-1)n_i(\mathbf{e}')\beta_i)\,\mathrm{e}(-(q-1)n_i(\mathbf{e})\beta_i) \\ &= \prod_{i=1}^{l} \mathrm{e}((q-1)(n_i(\mathbf{e}')-n_i(\mathbf{e}))\beta_i) = \mathrm{e}((q-1)\beta_j). \end{aligned}$$

We conclude that $(q-1)\beta_j \equiv 0 \mod 1$ for $j = 1, \ldots, n$.
By considering Corollary 2.4.8 for any admissible sequence, we note that (2.9) can only hold if

$$z = \mathrm{e}\left(-K + \sum_{j=1}^{n} n_j \cdot (q-1)\beta_j\right) = \mathrm{e}(-K).$$

□

We finally obtain the following theorem.

**Theorem 2.4.10.** *For any $m' \geq 2k$, there exists no $z \in \mathbb{U}$ such that (2.9) holds.*

*Proof.* By Lemma 2.4.9, we know that equality can just hold for $z = \mathrm{e}(-K)$.
We have already seen that for $\mathbf{d}' = (\delta, d_0, \ldots, d_{m-2})$ it follows that

$$M^{\mathbf{d}'}(z) = M^{\delta}(z)M^{\mathbf{d}}(z^q).$$

$\|.\|_\infty$ is sub-multiplicative and thus, for equality to hold, we need $z^q = \mathrm{e}(-K)$ for the second factor $(M^{\mathbf{d}}(z^q))$ as well as $z = \mathrm{e}(-K)$ for the product $(M^{\mathbf{d}'}(z))$, by Lemma 2.4.9. So we conclude $z = z^q = \mathrm{e}(-K)$. Therefore, we see that $z^q = \mathrm{e}(-qK) = \mathrm{e}(-K)$ which can just hold for $(q-1)K \equiv 0 \bmod 1$. This is equivalent to $(q-1)mK \equiv 0 \bmod m$. Since $mK \in \mathbb{Z}$ and $\gcd(q-1, m) = 1$, we know that $mK \equiv 0 \bmod m$ or $K \equiv 0 \bmod 1$ which yields a contradiction. □

# 3 Auxiliary Results

In this chapter, we present some auxiliary results which are used in Chapter 4, to prove the main theorem. For this proof, it is crucial to approximate characteristic functions of the intervals $[0, \alpha) \bmod 1$ where $0 \leq \alpha < 1$ by trigonometric polynomials. This is done by using Vaaler's method and Section 3.1 is dedicated to this step. As we deal with exponential sums we also use a generalization of Van-der-Corput's inequality which we prove in Section 3.2. In Section 3.3, we acquire some results dealing with sums of geometric series which we use to bound linear exponential sums. Section 3.4 is dedicated to one classic result on Gauss sums and allows us to find appropriate bounds on the occurring quadratic exponential sums in Chapter 4. The last section of this chapter deals with carry propagation. We find a quantitative statement that carry propagation along several digits is rare, i.e. exponentially decreasing.

## 3.1 Vaaler's method

The following theorem is a classical method to detect real numbers in an interval modulo 1 by means of exponential sums. For $\alpha \in \mathbb{R}$ with $0 \leq \alpha < 1$, we denote by $\chi_\alpha$ the characteristic function of the interval $[0, \alpha)$ modulo 1:

$$\chi_\alpha(x) = \lfloor x \rfloor - \lfloor x - \alpha \rfloor . \tag{3.1}$$

The main purpose of this section is to prove Theorem 3.1.1 by Vaaler [15].

**Theorem 3.1.1.** *For all $\alpha \in \mathbb{R}$ with $0 \leq \alpha < 1$ and all integer $H \geq 1$, there exist real-valued trigonometric polynomials $A_{\alpha,H}(x)$ and $B_{\alpha,H}(x)$ such that for all $x \in \mathbb{R}$*

$$|\chi_\alpha(x) - A_{\alpha,H}(x)| \leq B_{\alpha,H}(x). \tag{3.2}$$

*The trigonometric polynomials are defined by*

$$A_{\alpha,H}(x) = \sum_{|h| \leq H} a_h(\alpha, H)\, \mathrm{e}(hx), \;\; B_{\alpha,H}(x) = \sum_{|h| \leq H} b_h(\alpha, H)\, \mathrm{e}(hx), \tag{3.3}$$

*with coefficients $a_h(\alpha, H)$ and $b_h(\alpha, H)$ satisfying*

$$a_0(\alpha, H) = \alpha, \;\; |a_h(\alpha, H)| \leq \min\left(\alpha, \tfrac{1}{\pi|h|}\right), \;\; |b_h(\alpha, H)| \leq \tfrac{1}{H+1}. \tag{3.4}$$

In order to prove Theorem 3.1.1, we use the ideas and notation of Vaaler in [15]. We, therefore,

use the following specific functions:

$$H(z) := \left(\frac{\sin(\pi z)}{\pi}\right)^2 \left(\sum_{m=-\infty}^{\infty} \operatorname{sgn}(m)(z-m)^{-2} + 2z^{-1}\right)$$
$$J(z) := \frac{1}{2}H'(z)$$
$$K(z) := \left(\frac{\sin(\pi z)}{\pi z}\right)^2.$$

The definition of $H(z), K(z)$ was motivated by a related function

$$B(z) = H(z) + K(z)$$

which was considered by A. Beurling in the late 1930s. He observed that $B(z)$ is the unique entire function of exponential type $2\pi$ which fulfills $B(x) \geq \operatorname{sgn}(x)$ and minimizes $\int_{-\infty}^{\infty} B(x) - \operatorname{sgn}(x) dx$.

We find some important properties of these functions.

**Lemma 3.1.2.** *For all $x \in \mathbb{R}$,*

$$|H(x)| \leq 1$$
$$|\operatorname{sgn}(x) - H(x)| \leq K(x)$$

*holds.*

*Proof.* Since $H(x)$ and $\operatorname{sgn}(x)$ are odd functions it suffices to show that for all $x > 0$

$$1 - K(x) \leq H(x) \leq 1. \tag{3.5}$$

Assume $x > 0$ from now on. The identity

$$\sum_{m=-\infty}^{\infty} (z-m)^{-2} = \left(\frac{\pi}{\sin(\pi z)}\right)^2$$

on meromorphic functions $\mathbb{C} \to \mathbb{C}_\infty$ gives another representation of $H(x)$,

$$H(x) = 1 + \left(\frac{\sin(\pi x)}{\pi}\right)^2 \left(2x^{-1} - x^{-2} - 2\sum_{m=1}^{\infty} (x+m)^{-2}\right).$$

We use the arithmetic-geometric mean inequality to show the second inequality of Condition (3.5):

$$\begin{aligned} H(x) &= 1 + \left(\frac{\sin(\pi x)}{\pi}\right)^2 \left(2x^{-1} - x^{-2} - 2\sum_{m=1}^{\infty} (x+m)^{-2}\right) \\ &= 1 + \left(\frac{\sin(\pi x)}{\pi}\right)^2 \left(2x^{-1} - \left(\sum_{m=0}^{\infty} (x+m)^{-2} + (x+m+1)^{-2}\right)\right) \\ &\leq 1 + \left(\frac{\sin(\pi x)}{\pi}\right)^2 \left(2x^{-1} - 2\left(\sum_{m=0}^{\infty} (x+m)^{-1}(x+m+1)^{-1}\right)\right) \end{aligned}$$

By expansion into partial fractions we obtain a telescoping sum and yield

$$H(x) \leq 1 + \left(\frac{\sin(\pi x)}{\pi}\right)^2 (2x^{-1} - 2x^{-1}) = 1.$$

Next we show the first inequality of Condition (3.5):

$$\begin{aligned} H(x) &= 1 + \left(\frac{\sin(\pi x)}{\pi}\right)^2 \left(2x^{-1} - x^{-2} - 2\sum_{m=1}^{\infty} (x+m)^{-2}\right) \\ &\geq 1 + \left(\frac{\sin(\pi x)}{\pi}\right)^2 \left(2x^{-1} - x^{-2} - 2\sum_{m=0}^{\infty} (x+m)^{-1}(x+m+1)^{-1}\right) \\ &= 1 + \left(\frac{\sin(\pi x)}{\pi}\right)^2 (2x^{-1} - x^{-2} - 2x^{-1}) = 1 - K(x) \end{aligned}$$

□

We are now interested in the Fourier transform of $E(x) := H(x) - \operatorname{sgn}(x)$. We use the following definition of the Fourier transform and its inverse.

$$\begin{aligned} \widehat{F}(t) &= \int_{-\infty}^{\infty} \mathrm{e}(-tx) F(x) dx \\ F(x) &= \int_{-\infty}^{\infty} \mathrm{e}(tx) \widehat{F}(t) dt \end{aligned}$$

**Lemma 3.1.3.** *The function $x \in \mathbb{R} \mapsto J(x)$ satisfies*

$$J(x) \ll (1+|x|)^{-3}$$

*and is, therefore, integrable. Its Fourier transform is given by*

$$\widehat{J}(t) = \begin{cases} 1, & \text{if } t = 0 \\ \pi t(1-|t|)\cot(\pi t) + |t|, & \text{if } 0 < |t| < 1 \\ 0, & \text{if } |t| \geq 1 \end{cases}.$$

*Proof.* We define the partial sum of $H$:

$$H_N(z) = \left(\frac{\sin(\pi z)}{\pi}\right)^2 \left(\sum_{m=-N}^{N} \operatorname{sgn}(m)(z-m)^{-2} + 2z^{-1}\right).$$

It follows easily that

$$\lim_{N\to\infty} H_N(z) = H(z) \text{ and } \lim_{N\to\infty} \frac{1}{2} H_N'(z) = J(z)$$

uniformly on compact subsets of $\mathbb{C}$. Some analytic computations show that

$$\begin{aligned} K(z) &= \int_{-1}^{1} (1-|t|)\,\mathrm{e}(tz) dt \\ zK(z) &= \frac{1}{2\pi i} \int_{-1}^{1} \operatorname{sgn}(t)\,\mathrm{e}(tz) dt. \end{aligned}$$

We use these identities to rewrite $H_N(z)$,

$$\begin{aligned} H_N(z) &= \sum_{m=-N}^{N} \operatorname{sgn}(m) K(z-m) + 2zK(z) \\ &= \int_{-1}^{1} \sum_{m=-N}^{N} \operatorname{sgn}(m)(1-|t|)\,\mathrm{e}(-mt)\,\mathrm{e}(tz)dt + \frac{1}{i\pi}\int_{-1}^{1} \operatorname{sgn}(t)\,\mathrm{e}(tz)dt. \end{aligned}$$

We see that

$$\sum_{n=-N}^{N} \operatorname{sgn}(n)\,\mathrm{e}(-nt) = 2i\sum_{n=1}^{N} \sin(-2\pi nt) \overset{(*)}{=} -i\cot(\pi t) + i\frac{\cos(\pi(2N+1)t)}{\sin(\pi t)}$$

where Equality $(*)$ can be shown by induction on $N$. Applying $\frac{1}{2}\frac{d}{dz}$ to both sides, we see that

$$\begin{aligned} J(z) &= \frac{1}{2}\frac{d}{dz}\lim_{N\to\infty}\int_{-1}^{1}(1-|t|)\,\mathrm{e}(tz)\left(-i\cot(\pi t) + i\frac{\cos(\pi(2N+1)t)}{\sin(\pi t)}\right) + \frac{1}{i\pi}\operatorname{sgn}(t)\,\mathrm{e}(tz)dt \\ &= \int_{-1}^{1}((1-|t|)\pi t\cot(\pi t) + |t|)\,\mathrm{e}(tz)dt + \lim_{N\to\infty}\int_{-1}^{1}(1-|t|)t\frac{\cos(\pi(2N+1)t)}{\sin(\pi t)}\,\mathrm{e}(tz)dt, \end{aligned}$$

where

$$\lim_{N\to\infty}\int_{-1}^{1}(1-|t|)t\frac{\cos(\pi(2N+1)t)}{\sin(\pi t)}\,\mathrm{e}(tz)dt = 0$$

by the Riemann-Lebesgue Lemma. Therefore, we can identify the Fourier transform of $J(x)$. We define $\phi(t) = \pi t(1-t)\cot(\pi t) + t$ for $t \in [-1,2]\setminus\{0,1\}$ and defined at $0,1$ by continuity. We conclude that

$$J(z) = 2\int_0^1 \phi(t)\cos(2\pi tz)dt.$$

By iteratively integrating by parts three times we find

$$J(z) = \frac{1}{(2\pi z)^3}\left(2\int_0^1 \phi'''(t)\sin(2\pi tz)dt - \frac{4\pi^2}{3}\sin(2\pi z)\right).$$

This completes the proof, since $J(0)$ is bounded and $J(x) \ll x^{-3}$. □

Let $E$ be the function defined by $E(x) = H(x) - \operatorname{sgn}(x)$.

**Corollary 3.1.4.** *The fourier transform of $E$ is given by*

$$\widehat{E}(t) = \begin{cases} 0, & \text{if } t = 0 \\ (\pi it)^{-1}(\widehat{J}(t) - 1), & \text{if } t \neq 0 \end{cases}$$

*Proof.* We find that

$$\widehat{J}(t) - 1 = \frac{1}{2}\int_{-\infty}^{\infty} \mathrm{e}(-tx)dE(x).$$

By integrating by parts we find that

$$\frac{1}{2}\int_{-\infty}^{\infty}\mathrm{e}(-tx)dE(x) = \frac{2\pi it}{2}\int_{-\infty}^{\infty}\mathrm{e}(-tx)E(x)dx = \frac{1}{\pi it}\widehat{E}(t).$$

□

The functions mentioned above were used in [15] to approximate characteristic functions of intervalls $[a,b]$ in $\mathbb{R}$.

For the periodic case he introduced some related functions. Therefore he needed the following definition.

**Definition 3.1.5.** Let $F$ be any of the functions above. We define $F_\delta(x) := \delta F(\delta x)$.

One computes easily that $\widehat{F_\delta}(x) = \widehat{F}(\delta^{-1}x)$ and we define

$$j_N(x) := \sum_{m=-\infty}^{\infty} J_{N+1}(x+m) = \sum_{n=-\infty}^{\infty} \widehat{J}_{N+1}(n)\,\mathrm{e}(nx) = \sum_{n=-N}^{N} \widehat{J}_{N+1}(n)\,\mathrm{e}(nx),$$
$$k_N(x) := \sum_{m=-\infty}^{\infty} K_{N+1}(x+m) = \sum_{n=-\infty}^{\infty} \widehat{K}_{N+1}(n)\,\mathrm{e}(nx) = \sum_{n=-N}^{N} \widehat{K}_{N+1}(n)\,\mathrm{e}(nx).$$

The second equalities hold by Poisson's summation formula and the third equalities hold since $\widehat{J}_{N+1}(n) = \widehat{K}_{N+1}(n) = 0$ if $|n| \geq N+1$.

Furthermore we define

$$\psi(x) = \begin{cases} x - \lfloor x \rfloor - \frac{1}{2}, & \text{if } x \notin \mathbb{Z} \\ 0, & \text{if } x \in \mathbb{Z} \end{cases} \tag{3.6}$$

and denote by

$$f * g(x) = \int_{-1/2}^{1/2} f(x-\xi)g(\xi)d\xi$$

the convolution of two periodic functions $f, g$ with period 1 and by

$$\widehat{f}(n) = \int_{-1/2}^{1/2} f(x)\,\mathrm{e}(-nx)dx$$

the $n$-th Fourier coefficient of $f$.

**Lemma 3.1.6.** *For any $x \in \mathbb{R}$*

$$\frac{d}{dx}(\psi * j_N(x)) = 1 - j_N(x) \tag{3.7}$$

*and*

$$|\psi * j_N(x) - \psi(x)| \leq (2N+2)^{-1} k_N(x).$$

*hold.*

*Proof.* An easy computation yields

$$\psi * j_N(x) = \sum_{n=-N}^{N} \widehat{J}_{N+1}(n)(\mathrm{e}(n\,\cdot\,) * \phi(.))(x) = -\sum_{\substack{n=-N \\ n\neq 0}}^{N} \widehat{J}_{N+1}(n)\,\mathrm{e}(nx)\frac{1}{2\pi i n}.$$

Differentiation yields Equation (3.7). We find by Poisson's summation formula and Corollary 3.1.4 that

$$\begin{aligned}(2N+2)^{-1}\sum_{m=-\infty}^{\infty} E_{N+1}(x+m) &= (2N+2)^{-1}\sum_{n=-\infty}^{\infty}\widehat{E}_{N+1}(n)\,\mathrm{e}(nx)\\ &= \sum_{\substack{n=-\infty\\ n\neq 0}}^{\infty}(2\pi i n)^{-1}(\widehat{J}(n)-1)\,\mathrm{e}(nx) = \psi * j_N(x) - \psi(x)\end{aligned}$$

Using Lemma 3.1.2, we yield

$$|\psi * j_N(x) - \psi(x)| \leq (2N+2)^{-1}\sum_{m=-\infty}^{\infty} K_{N+1}(x+m) = (2N+2)^{-1}k_N(x). \qquad \square$$

We call a function $f:\mathbb{R}\to\mathbb{C}$ *normalized* if for all $x\in\mathbb{R}$

$$f(x) = \lim_{t\to 0+}\frac{1}{2}(f(x+t)+f(x-t))$$

holds. Note that $\chi_\alpha$ is obviously not normalized.

We denote with $V_f$ the total variation of $f$ on $[-\frac{1}{2},\frac{1}{2}]$ and with $V_f(x)$ the total variation of $f$ on $[-\frac{1}{2},x]$. There obviously holds $V_f = V_f(\frac{1}{2})$. We write $dV_f * k_N$ for the convolution

$$(dV_f) * k_N(x) = \int_{-1/2}^{1/2} k_n(x-\xi)dV_f(\xi).$$

We are now ready to proof one of the main results of [15].

**Theorem 3.1.7.** *Let $f$ be a normalized function $f:\mathbb{R}\to\mathbb{C}$ with bounded variation on any interval of length 1. Then $f * j_N(x)$ and $(dV_f) * k_N(x)$ are trigonometric polynomials of degree at most $N$ which satisfy*

$$|f(x) - f * j_N(x)| \leq (2N+2)^{-1}(dV_f) * k_N(x). \tag{3.8}$$

*Proof.* For all continuity points $x$ of $f$ we see by Equation (3.7) that

$$\begin{aligned}&\int_{-1/2}^{1/2} f(x-\xi)d(\psi * j_N(\xi) - \psi(\xi))\\ &\qquad = \int_{-1/2}^{1/2} f(x-\xi)(1-j_N(\xi))d\xi - \int_{-1/2}^{1/2} f(x-\xi)d\psi(\xi)\\ &\qquad = f(x) - f * j_N(x).\end{aligned}$$

Integrating the left side of the equation above by parts yields again at all continuity points $x$ of $f$,

$$f(x) - f * j_N(x) = \int_{-1/2}^{1/2} \psi * j_N(x-\xi) - \psi(x-\xi)df(\xi).$$

Since $f$ is continuous almost everywhere, we conclude

$$\begin{aligned}|f(x) - f * j_N(x)| &\leq \int_{-1/2}^{1/2} |\psi * j_N(x-\xi) - \psi(x-\xi)| dV_f(\xi) \\ &\leq (2N+2)^{-1} \int_{-1/2}^{1/2} k_N(x-\xi) dV_f(\xi) \\ &= (2N+2)^{-1} (dV_f) * k_N(x).\end{aligned}$$

Since $f$ is normalized, we conclude that Inequality (3.8) holds for all $x \in \mathbb{R}$. □

We are now prepared to prove Theorem 3.1.1.

*Proof (by [4]).* In order to apply Theorem 3.1.7, we have to normalize $\chi_\alpha(x)$:

$$\widetilde{\chi_\alpha}(x) := \lim_{t \to 0_+} \frac{1}{2}(\chi_\alpha(x+t) + \chi_\alpha(x-t))$$

By Theorem 3.1.7 we find trigonometric polynomials $A_{\alpha,H}(x) = \widetilde{\chi}_\alpha * j_H(x)$, $B_{\alpha,H}(x) = (2N+2)^{-1}(dV_f) * k_H(x)$ satisfying

$$|\widetilde{\chi_\alpha}(x) - A_{\alpha,H}(x)| \leq B_{\alpha,H}(x).$$

One computes by Lemma 3.1.3,

$$\begin{aligned}\widetilde{\chi_\alpha} * j_H(x) &= \sum_{h=-H}^{H} \widehat{J}_{H+1}(h) (\mathrm{e}(h\,\cdot) * \widetilde{\chi_\alpha})(x) \\ &= \sum_{h=-H}^{H} \widehat{J}_{H+1}(h) \frac{1}{2\pi i h} (\mathrm{e}(hx) - \mathrm{e}(h(x-\alpha))) \\ &= \sum_{h=-H}^{H} \mathrm{e}(hx)\, \mathrm{e}\left(-\frac{h\alpha}{2}\right) \underbrace{\frac{\sin(\pi\alpha h)}{h\pi} \left(\pi \frac{h}{H+1}\left(1 - \frac{|h|}{H+1}\right) \cot\left(\frac{\pi|h|}{H+1}\right) + \frac{|h|}{H+1}\right)}_{:= a'_h(\alpha,H)}.\end{aligned}$$

and thus

$$A_{\alpha,H}(x) = \sum_{|h| \leq H} \mathrm{e}(hx)\, \mathrm{e}\left(-\frac{h\alpha}{2}\right) a'_h(\alpha, H)$$

where $a'_h(\alpha, H) \in \mathbb{R}$. A quick calculation shows that $A_{\alpha,H}(x)$ is real-valued:

$$\begin{aligned}a'_h(\alpha, H) &= a'_{-h}(\alpha, H) \\ A_{\alpha,H}(x) &= \alpha + \sum_{h=1}^{H} a'_h(\alpha, H) \left(\mathrm{e}\left(h\left(x - \frac{\alpha}{2}\right)\right) + \mathrm{e}\left(-h\left(x - \frac{\alpha}{2}\right)\right)\right) \\ &= \alpha + \sum_{h=1}^{H} 2a'_h(\alpha, H) \cos\left(2\pi h \left(x - \frac{\alpha}{2}\right)\right).\end{aligned}$$

To show $|a_h(\alpha, H)| \leq \min\left(\alpha, \frac{1}{\pi|h|}\right)$, we observe that

$$a_h(\alpha, H) = \mathrm{e}\left(-\frac{h\alpha}{2}\right)\frac{\sin(\pi h\alpha)}{\pi h}\phi\left(\frac{|h|}{H+1}\right)$$

with $\phi$ defined as in the proof of Lemma 3.1.3. Since $\left|\frac{\sin(\pi h\alpha)}{\pi h}\right| \leq \min\left(\alpha, \frac{1}{\pi|h|}\right)$ it is sufficient to note that $\phi$ is non-negative and strictly decreasing on $[0,1]$, which is easily verifiable by differentiating.
Similarly one sees that

$$B_{\alpha,H}(x) = \sum_{|h|\leq H} \mathrm{e}(hx)\,\mathrm{e}\left(-\frac{h\alpha}{2}\right)\frac{1}{H+1}\left(1-\frac{|h|}{H+1}\right)\cos(\pi h\alpha).$$

This completes the proof of Theorem 3.1.1 □

Using this method we can detect points in a $d$-dimensional box (modulo 1):

**Lemma 3.1.8.** *For $(\alpha_1, \ldots, \alpha_d) \in [0,1)^d$ and $(H_1, \ldots, H_d) \in \mathbb{N}^d$ with $H_1 \geq 1, \ldots, H_d \geq 1$, we have for all $(x_1, \ldots, x_d) \in \mathbb{R}^d$*

$$\left|\prod_{j=1}^{d}\chi_{\alpha_j}(x_j) - \prod_{j=1}^{d}A_{\alpha_j,H_j}(x_j)\right| \leq \sum_{\emptyset\neq J\subseteq\{1,\ldots,d\}}\prod_{j\notin J}\chi_{\alpha_j}(x_j)\prod_{j\in J}B_{\alpha_j,H_j}(x_j) \tag{3.9}$$

*where $A_{\alpha,H}(.)$ and $B_{\alpha,H}(.)$ are the real valued trigonometric polynomials defined by* (3.3).

*Proof (by [7]).* We have

$$\left|\prod_{j=1}^{d}\chi_{\alpha_j}(x_j) - \prod_{j=1}^{d}A_{\alpha_j,H_j}(x_j)\right| \leq \sum_{\emptyset\neq J\subseteq\{1,\ldots,d\}}\prod_{j\notin J}\left|\chi_{\alpha_j}(x_j)\right|\prod_{j\in J}\left|\chi_{\alpha_j}(x_j) - A_{\alpha_j,H_j}(x_j)\right|$$

Since $\chi_{\alpha_i} \geq 0$ and (3.2), we get (3.9). □

Let $(U_1, \ldots, U_d) \in \mathbb{N}^d$ with $U_1 \geq 1, \ldots, U_d \geq 1$ and define $\alpha_1 = 1/U_1, \ldots, \alpha_d = 1/U_d$. For $j = 1, \ldots, d$ and $x \in \mathbb{R}$ we have

$$\sum_{0\leq u_j<U_j}\chi_{\alpha_j}\left(x - \frac{u_j}{U_j}\right) = 1. \tag{3.10}$$

Let $N \in \mathbb{N}$ with $N \geq 1$, $f : \{1, \ldots, N\} \to \mathbb{R}^d$ and $g : \{1, \ldots, N\} \to \mathbb{C}$ such that $|g| \leq 1$. If $f = (f_1, \ldots, f_n)$, we can express the sum

$$S = \sum_{n=1}^{N} g(n)$$

as

$$S = \sum_{n=1}^{N} g(n)\sum_{0\leq u_1<U_1}\chi_{\alpha_1}\left(f_1(n) - \frac{u_1}{U_1}\right)\cdots\sum_{0\leq u_d<U_d}\chi_{\alpha_d}\left(f_d(n) - \frac{u_d}{U_d}\right).$$

We now define $(H_1, \dots, H_d) \in \mathbb{N}^d$ with $H_1 \geq 1, \dots, H_d \geq 1$,

$$\widetilde{S} = \sum_{n=1}^{N} g(n) \sum_{0 \leq u_1 < U_1} A_{\alpha_1, H_1}\left(f_1(n) - \frac{u_1}{U_1}\right) \cdots \sum_{0 \leq u_d < U_d} A_{\alpha_d, H_d}\left(f_d(n) - \frac{u_d}{U_d}\right).$$

**Lemma 3.1.9.** *With the notations from above, we have*

$$\left|S - \widetilde{S}\right| \leq \sum_{\ell=1}^{d-1} \sum_{1 \leq j_1 < \cdots < j_\ell} \frac{U_{j_1} \cdots U_{j_\ell}}{H_{j_1} \cdots H_{j_\ell}} \sum_{|h_{j_1}| \leq H_{j_1}/U_{j_1}} \cdots \sum_{|h_{j_\ell}| \leq H_{j_\ell}/U_{j_\ell}} \left|\sum_{n=1}^{N} \mathrm{e}\left(h_{j_1} U_{j_1} f_{j_1}(n) + \cdots + h_{j_\ell} U_{j_\ell} f_{j_\ell}(n)\right)\right|. \tag{3.11}$$

*Proof (by [7]).* By (3.9), we have

$$\left|S - \widetilde{S}\right| \leq \sum_{n=1}^{N} |g(n)| \sum_{\emptyset \neq J \subseteq \{1,\dots,d\}} \left(\prod_{j \notin J} \sum_{0 \leq u_j < U_j} \chi_{\alpha_j}\left(f_j(n) - \frac{u_j}{U_j}\right)\right) \cdot \left(\prod_{j \in J} \sum_{0 \leq u_j < U_j} B_{\alpha_j, H_j}\left(f_j(n) - \frac{u_j}{U_j}\right)\right)$$

which by (3.10) gives

$$\left|S - \widetilde{S}\right| \leq \sum_{n=1}^{N} |g(n)| \sum_{\emptyset \neq J \subseteq \{1,\dots,d\}} \prod_{j \in J} \sum_{0 \leq u_j < U_j} B_{\alpha_j, H_j}\left(f_j(n) - \frac{u_j}{U_j}\right).$$

Since $B_{\alpha_j, H_j} \geq 0$ and $|g| \leq 1$, we conclude

$$\left|S - \widetilde{S}\right| \leq \sum_{\emptyset \neq J \subseteq \{1,\dots,d\}} \sum_{n=1}^{N} \prod_{j \in J} \sum_{0 \leq u_j < U_j} \sum_{|h_j| \leq H_j} b_{h_j}(\alpha_j, H_j)\, \mathrm{e}\left(h_j f_j(n) - \frac{h_j u_j}{U_j}\right).$$

Observing that

$$\sum_{0 \leq u_j < U_j} \mathrm{e}\left(-\frac{h_j u_j}{U_j}\right) = \begin{cases} U_j & \text{if } h_j \equiv 0 \bmod U_j \\ 0 & \text{otherwise} \end{cases}$$

we obtain

$$\left|S - \widetilde{S}\right| \leq \sum_{\emptyset \neq J \subseteq \{1,\dots,d\}} \sum_{n=1}^{N} \prod_{j \in J} U_j \sum_{0 \leq u_j < U_j} \sum_{|h_j| \leq H_j/U_j} b_{h_j U_j}(\alpha_j, H_j)\, \mathrm{e}\left(h_j U_j f_j(n)\right).$$

Expanding the product, reversing the order of summations and using (3.4) leads to (3.11). □

## 3.2 Van-der-Corput's inequality

The following lemma is a generalization of Van-der-Corput's inequality.

**Lemma 3.2.1.** *For all complex numbers $z_1, \dots, z_N$ and all integers $Q \geq 1$ and $R \geq 1$, we have*

$$\left| \sum_{1 \leq n \leq N} z_n \right|^2 \leq \frac{N + QR - Q}{R} \left( \sum_{1 \leq n \leq N} |z_n|^2 + 2 \sum_{1 \leq r < R} \left(1 - \frac{r}{R}\right) \sum_{1 \leq n \leq N-Qr} \Re\left(z_{n+Qr} \overline{z_n}\right) \right) \tag{3.12}$$

*where $\Re(z)$ denotes the real part of $z \in \mathbb{C}$.*

*Proof (by [5]).* We set $z_n = 0$ for $n \leq 0$ or $n > N$ and use the following identity,

$$R \sum_{n=1}^{N} z_n = R \sum_{n} z_n = \sum_{r=0}^{R-1} \sum_{n} z_{n+Qr} = \sum_{n} \sum_{r=0}^{R-1} z_{n+Qr}.$$

where each of the sums is actually finite. The summands in the inner sum vanish if $n + Qr \notin \{1, \dots, N\}$ for all $0 \leq r \leq R-1$. Therefore, we can bound the values of $n$ by $1 - Q(R-1) \leq n \leq N$ and thus there are at most $N + Q(R-1)$ non-vanishing summands. By applying the Cauchy-Schwarz inequality, one finds

$$\begin{aligned}
R^2 \left| \sum_{n} z_n \right|^2 &= \left| \sum_{n=1-Q(R-1)}^{N} 1 \cdot \sum_{r=0}^{R-1} z_{n+Qr} \right|^2 \leq (N + Q(R-1)) \sum_{n} \left| \sum_{r=0}^{R-1} z_{n+Qr} \right|^2 \\
&\leq (N + Q(R-1)) \sum_{n} \sum_{r_1=0}^{R-1} \sum_{r_2=0}^{R-1} z_{n+Qr_1} \overline{z_{n+Qr_2}} \\
&= (N + Q(R-1)) \sum_{r_1=0}^{R-1} \sum_{r_2=0}^{R-1} \sum_{m} z_{m+Q(r_1-r_2)} \overline{z_m} \\
&= (N + Q(R-1)) \sum_{r=-R}^{R} (R - |r|) \sum_{m} z_{m+Qr} \overline{z_m} \\
&= (N + Q(R-1))(R \sum_{n=1}^{N} |z_n|^2 + 2 \sum_{r=1}^{R-1} (R-r) \sum_{n=1}^{N-Qr} \Re(z_{n+Qr} \overline{z_n})).
\end{aligned}$$

Dividing both sides by $R^2$ yields the desired result. □

## 3.3 Sums of geometric series

We will often make use of the following upper bound for geometric series with ratio $\mathrm{e}(\xi), \xi \in \mathbb{R}$ and $L_1, L_2 \in \mathbb{Z}$, $L_1 \leq L_2$:

$$\left| \sum_{L_1 < \ell \leq L_2} \mathrm{e}(\ell \xi) \right| \leq \min(L_2 - L_1, |\sin \pi \xi|^{-1}), \tag{3.13}$$

which is obtained from the formula for finite geometric series.

The following results allow us to find useful estimates for special double and triple sums involving geometric series.

**Lemma 3.3.1.** *Let $(a,m) \in \mathbb{Z}^2$ with $m \geq 1$, $\delta = \gcd(a,m)$ and $b \in \mathbb{R}$. For any real number $U > 0$, we have*

$$\sum_{0 \leq n \leq m-1} \min\left(U, \left|\sin\left(\pi \tfrac{an+b}{m}\right)\right|^{-1}\right) \leq \delta \min\left(U, \left|\sin\left(\pi \tfrac{\delta \|b/\delta\|}{m}\right)\right|^{-1}\right) + \frac{2\,m}{\pi}\log(2\,m). \quad (3.14)$$

*Proof (by [5] and [7]).* The result is trivial for $m = 1$ and $\delta = m$. Hence we assume $d \neq m$ and consequently $1 \leq d \leq \frac{m}{2}$. Let $a = a'd, m = m'd, b = b'd + r$ with $a', b' \in \mathbb{Z}, m' \in \mathbb{N}, r \in \mathbb{R}, -\frac{d}{2} < r \leq \frac{d}{2}$ and

$$S = \sum_{n=0}^{m-1} \min\left(U, \left|\sin\left(\pi \frac{an+b}{m}\right)\right|^{-1}\right) = \sum_{n=0}^{m-1} \min\left(U, \left|\sin\left(\frac{\pi}{m'}(a'n + b' + \frac{r}{\delta})\right)\right|^{-1}\right).$$

Since $\gcd(a', m') = 1$ we know that $a'n + b' = x \bmod m'$ has exactly $\delta$ solutions for $0 \leq n \leq m-1$. Hence

$$S = \delta \sum_{n=0}^{m'-1} \min\left(U, \left|\sin\left(\frac{\pi}{m'}\left(n + \frac{r}{\delta}\right)\right)\right|^{-1}\right).$$

We want to drop the absolute value: The argument is negative if $n + \frac{r}{\delta} < 0$ which can only happen for $r < 0$. In this case we exchange $r$ by $-r$, $n$ by $-n$ and change the order of summation. Thus we can assume that $0 \leq n + \frac{r}{\delta} < m'$ and, therefore, drop the absolute value and find

$$\begin{aligned} S = \delta \min\left(U, \sin\left(\frac{\pi r}{m'd}\right)^{-1}\right) + \delta \min\left(U, \sin\left(\frac{\pi}{m'}\left(1 - \frac{r}{d}\right)\right)^{-1}\right) \\ + \delta \sum_{n=1}^{m'-2} \min\left(U, \sin\left(\frac{\pi}{m'}\left(n + \frac{r}{d}\right)\right)^{-1}\right). \end{aligned}$$

Since $t \mapsto (\sin t)^{-1}$ is a convex function on $(0, \pi)$, we find

$$S \leq \delta \min\left(U, \sin\left(\frac{\pi r}{m'd}\right)^{-1}\right) + \delta \sin\left(\frac{\pi}{m'}\left(1 - \frac{r}{d}\right)\right)^{-1} + \delta \int_{1/2}^{m'-3/2} \sin\left(\frac{\pi}{m'}\left(t + \frac{r}{d}\right)\right)^{-1} dt.$$

Let

$$h(x) := \sin\left(\frac{\pi}{m'}(1-x)\right)^{-1} + \int_{1/2}^{m'-3/2} \sin\left(\frac{\pi}{m'}(t+x)\right)^{-1} dt.$$

By noting that $t \mapsto \sin(t)^{-1}$ is convex on $(0, \pi)$, it follows directly that $h$ is convex on $[0, 1/2]$ and, therefore, attains its maximum on a boundary point. Next we show that the maximum is

obtained at $\frac{1}{2}$:

$$\begin{aligned} h\left(\frac{1}{2}\right) - h(0) &= \sin\left(\frac{\pi}{2m'}\right)^{-1} - \sin\left(\frac{\pi}{m'}\right)^{-1} + \int_{m'-3/2}^{m'-1} \sin\left(\frac{\pi}{m'}t\right)^{-1} dt - \int_{1/2}^{1} \sin\left(\frac{\pi}{m'}t\right)^{-1} dt \\ &\geq \sin\left(\frac{\pi}{2m'}\right)^{-1} - \sin\left(\frac{\pi}{m'}\right)^{-1} + \frac{1}{2}\sin\left(\frac{3\pi}{2m'}\right)^{-1} - \frac{1}{2}\sin\left(\frac{\pi}{2m'}\right)^{-1} \\ &= \frac{1}{2}\left(\sin\left(\frac{\pi}{2m'}\right)^{-1} + \sin\left(\frac{3\pi}{2m'}\right)^{-1}\right) - \sin\left(\frac{\pi}{m'}\right)^{-1} \geq 0. \end{aligned}$$

Where the last inequality holds by convexity. Hence $h$ indeed attains it maximum at $\frac{1}{2}$. We yield

$$S \leq \delta \min\left(U, \sin\left(\frac{\pi r}{m'd}\right)^{-1}\right) + \delta \sin\left(\frac{\pi}{2m'}\right)^{-1} + \delta \int_{1}^{m'-1} \sin\left(\frac{\pi t}{m'}\right)^{-1} dt.$$

To compute the integral, we note that $(\log\tan\frac{t}{2})' = \sin(t)^{-1}$:

$$S \leq \delta \min\left(U, \sin\left(\frac{\pi r}{m'd}\right)^{-1}\right) + \delta \sin\left(\frac{\pi}{2m'}\right)^{-1} + 2\frac{m'd}{\pi}\log\cot\frac{\pi}{2m'}$$

Since $0 \leq \frac{b}{d} - b' = \frac{r}{d} \leq \frac{1}{2}$, we can identify $\frac{r}{d} = ||\frac{b}{d}||$. Using $\cot\left(\frac{\pi}{2m'}\right) \leq \frac{2m'}{\pi}$ and the fact that $\sin(x)$ is concave on $[0,\pi]$, we observe:

$$\begin{aligned} \delta\sin(\frac{\pi}{2m'})^{-1} + \frac{2m'\delta}{\pi}\log\cot\frac{\pi}{2m'} &\leq \delta\sin(\frac{\pi}{2m'})^{-1} + \frac{2m'\delta}{\pi}\log\frac{2m'}{\pi} \\ &\leq \sin(\frac{\pi}{2\delta m'})^{-1} + \frac{2m'\delta}{\pi}\log\frac{2m'\delta}{\pi} \leq \frac{2m'\delta}{\pi}\log(2m'\delta) \end{aligned}$$

For $m = m'\delta \geq 2$ which holds by assumption. □

**Lemma 3.3.2.** *Let $m \geq 1$ and $A \geq 1$ be integers and $b \in \mathbb{R}$. For any real number $U > 0$, we have*

$$\frac{1}{A}\sum_{1\leq a\leq A}\sum_{0\leq n<m} \min\left(U, \left|\sin\left(\pi\tfrac{an+b}{m}\right)\right|^{-1}\right) \ll \tau(m)\ U + m\log m \tag{3.15}$$

*and, if $|b| \leq \frac{1}{2}$, we have an even sharper bound*

$$\frac{1}{A}\sum_{1\leq a\leq A}\sum_{0\leq n<m} \min\left(U, \left|\sin\left(\pi\tfrac{an+b}{m}\right)\right|^{-1}\right) \ll \tau(m)\min\left(U, \left|\sin\left(\pi\tfrac{b}{m}\right)\right|^{-1}\right) + m\log m, \tag{3.16}$$

*where $\tau(m)$ denotes the number of divisors of $m$.*

*Proof (by [7]).* Using (3.14) we have for all $b \in \mathbb{R}$, that

$$\sum_{0\leq n<m} \min\left(U, \left|\sin\left(\pi\tfrac{an+b}{m}\right)\right|^{-1}\right) \ll \gcd(a,m)\ U + m\log m.$$

Since $\gcd(a,m)\,\|b/\gcd(a,m)\| = |b|$ for $|b| \leq \frac{1}{2}$, this can be sharpened using (3.14) to

$$\sum_{0\leq n<m} \min\left(U, \left|\sin\left(\pi\tfrac{an+b}{m}\right)\right|^{-1}\right) \ll \gcd(a,m)\min\left(U, \left|\sin\left(\pi\tfrac{b}{m}\right)\right|^{-1}\right) + m\log m.$$

By observing that

$$\sum_{1\le a\le A}\gcd(a,m)=\sum_{\substack{d\mid m\\ d\le A}}d\sum_{\substack{1\le a\le A\\ \gcd(a,m)=d}}1\le\sum_{\substack{d\mid m\\ d\le A}}d\sum_{\substack{1\le a\le A\\ d\mid a}}1=\sum_{\substack{d\mid m\\ d\le A}}d\left\lfloor\frac{A}{d}\right\rfloor\le A\,\tau(m), \tag{3.17}$$

we immediately get (3.15) and (3.16). □

## 3.4 Gauss sums

In the proof of the main theorem, we will meet quadratic exponential sums. We first consider Gauss sums $\mathrm{G}(a,b;m)$ which are defined by:

$$\mathrm{G}(a,b;m):=\sum_{n=0}^{m-1}\mathrm{e}\left(\frac{an^2+bn}{m}\right).$$

In this chapter, we want to prove one classic result on Gauss sums, namely Theorem 3.4.1.

**Theorem 3.4.1.** *For all $(a,b,m)\in\mathbb{Z}^3$ with $m\ge 1$,*

$$\left|\sum_{n=0}^{m-1}\mathrm{e}\left(\tfrac{an^2+bn}{m}\right)\right|\le\sqrt{2m\gcd(a,m)} \tag{3.18}$$

*holds.*

To prove Theorem 3.4.1, we simplify the expressions step by step following [16]. At first, we relate $\mathrm{G}(a,b;m)$ to some $\mathrm{G}(a',b';m')$ with $\gcd(a',m')=1$.

**Lemma 3.4.2.** *Let $d:=\gcd(a,m)$.*

1. *If $d\mid b$, then $\mathrm{G}(a,b;m)=d\,\mathrm{G}(a/d,b/d;m/d)$.*
2. *If $d\nmid b$, then $\mathrm{G}(a,b;m)=0$.*

*Proof.* Using $m'=m/d, a'=a/d$ and the fact that $dm'\mid(2da'km'r+da'k^2m'^2)$ and $\mathrm{e}(x)=\mathrm{e}(y)$ if $x\equiv y \bmod 1$, we see that,

$$\begin{aligned}\mathrm{G}(a,b;m)&=\sum_{r=0}^{m'-1}\sum_{k=0}^{d-1}\mathrm{e}\left(\frac{da'(km'+r)^2+b(km'+r)}{dm'}\right)\\&=\sum_{r=0}^{m'-1}\mathrm{e}\left(\frac{a'r^2}{m'}+\frac{br}{dm'}\right)\sum_{k=0}^{d-1}\mathrm{e}\left(\frac{bk}{d}\right).\end{aligned}$$

Since

$$\sum_{k=0}^{d-1}\mathrm{e}\left(\frac{bk}{d}\right)=\begin{cases}d, & \text{for } d\mid b\\ 0, & \text{for} d\nmid b\end{cases}$$

the desired results follow directly. □

As we have seen that $d \nmid b$ implies $\mathrm{G}(a,b;m) = 0$, we now assume that $d \mid b$ and define $b' = b/d$. We have seen above that $\mathrm{G}(a,b;m) = d\ \mathrm{G}(a',b';m')$. Therefore it is easy to see that it is sufficient to show that $\mathrm{G}(a,b;m) \leq \sqrt{2m}$ for $\gcd(a,m) = 1$ in order to prove Theorem 3.4.1.

Next, we want to reduce the problem to $b = 0$ or $b = 1$.

**Lemma 3.4.3.** *Let $\overline{a}$ denote the multiplicative inverse of $a \bmod m$ (i.e. $a\overline{a} = 1 \bmod m$).*

*(1) If $m$ is odd, it follows that*

$$\mathrm{G}(a,b;m) = \mathrm{e}\left(-\frac{\overline{a}b^2}{4m}\right)\mathrm{G}(a,0;m).$$

*(2) If $b$ is even, it follows that*

$$\mathrm{G}(a,b;m) = \mathrm{e}\left(-\frac{\overline{a}}{m}\frac{b^2}{4}\right)\mathrm{G}(a,0;m).$$

*(3) If $b$ is odd, it follows that*

$$\mathrm{G}(a,b;m) = \mathrm{e}\left(-\frac{\overline{a}}{m}\frac{b^2-1}{4}\right)\mathrm{G}(a,1;m).$$

*Proof.* We shift $n \mapsto n + c$ with $c \in \mathbb{Z}$. This just changes the order of summation since e is a periodic function with period 1. Thus one yields

$$\begin{aligned}\mathrm{G}(a,b;m) &= \sum_{n=0}^{m-1} \mathrm{e}\left(\frac{an^2}{m}\right)\mathrm{e}\left(\frac{2anc}{m} + \frac{ac^2}{m} + \frac{bn}{m} + \frac{bc}{m}\right)\\ &= \sum_{n=0}^{m-1} \mathrm{e}\left(\frac{an^2}{m}\right)\mathrm{e}\left(n\frac{2ac+b}{m} + \frac{ac^2+bc}{m}\right).\end{aligned}$$

By choosing $c = -\overline{2a}b$ for (1), one finds that $2ac + b \equiv 0 \bmod m$ and the first result follows.
For (2), we choose $c = -\frac{b}{2}\overline{a}$ and find again that $2ac + b \equiv 0 \bmod m$.
For (3), we choose $c = -\frac{b-1}{2}\overline{a}$ and find that $2ac + b \equiv 1 \bmod m$. □

**Lemma 3.4.4.** *If $\gcd(m,n) = 1$ then*

$$\mathrm{G}(a,b;mn) = \mathrm{G}(an,b;m)\,\mathrm{G}(am,b;n).$$

*Proof.* By the Extended Euclidean Algorithm, we know that for every $k$ we can find unique $k_1 \bmod m$ and $k_2 \bmod n$ such that $k \equiv nk_1 + mk_2 \bmod mn$. We conclude

$$\begin{aligned}\mathrm{G}(a,b;mn) &= \sum_{k=0}^{mn-1} \mathrm{e}\left(\frac{ak^2+bk}{mn}\right)\\ &= \sum_{k_1=0}^{m-1}\sum_{k_2=0}^{n-1} \mathrm{e}\left(\frac{a(nk_1+mk_2)^2 + b(nk_1+mk_2)}{mn}\right)\\ &= \sum_{k_1=0}^{m-1} \mathrm{e}\left(\frac{ank_1^2+bk_1}{m}\right)\sum_{k_2=0}^{n-1} \mathrm{e}\left(\frac{amk_2^2+bk_2}{n}\right)\\ &= \mathrm{G}(an,b;m)\,\mathrm{G}(am,b;n).\end{aligned}$$

Thus the result is proven. □

Thus we can reduce the computation of $\mathrm{G}(a,b;m)$ to $\mathrm{G}(a,b;p^\alpha)$ where $p$ is a prime number. The next step is to reduce the exponent $\alpha$.

**Lemma 3.4.5.** *If $p$ is an odd prime number and $\alpha \geq 2$, then $\mathrm{G}(a,0;p^\alpha) = p\,\mathrm{G}(a,0;p^{\alpha-2})$.*

*Proof.* We compute $\mathrm{G}(a,0;p^\alpha)$

$$\sum_{j=0}^{p-1}\sum_{k=0}^{p^{\alpha-1}-1} \mathrm{e}\left(\frac{a(jp^{\alpha-1}+k)^2}{p^\alpha}\right) = \sum_{k=0}^{p^{\alpha-1}-1} \mathrm{e}\left(\frac{ak^2}{p^\alpha}\right)\sum_{j=0}^{p-1}\mathrm{e}\left(\frac{2ajk}{p}\right).$$

As the inner sum is 0 for $p \nmid k$ and $p$ otherwise, the result follows immediately. □

Unfortunately there is one piece that was not covered in [16]:

**Lemma 3.4.6.** *For $\alpha \geq 4$ and $a \in \mathbb{Z}$,*

$$\mathrm{G}(a,0;2^\alpha) = 2\,\mathrm{G}(a,0;2^{\alpha-2})$$

*and $\mathrm{G}(a,0;2) = 0, \mathrm{G}(a,0;4) = 2 + 2\,\mathrm{e}\left(\frac{a}{4}\right), \mathrm{G}(a,0;8) = 4\,\mathrm{e}\left(\frac{a}{8}\right)$ hold.*

*Proof.* We find that by using $\sum_{j=0}^{3}\mathrm{e}(akj/2) = 4\cdot\mathbf{1}_{2\mid k}$

$$\begin{aligned}
\mathrm{G}(a,0;2^\alpha) &= \sum_{k=0}^{2^{\alpha-2}-1}\sum_{j=0}^{3}\mathrm{e}\left(\frac{a(k+j2^{\alpha-2})^2}{2^\alpha}\right) = \sum_{k=0}^{2^{\alpha-2}-1}\mathrm{e}\left(\frac{ak^2}{2^\alpha}\right)\sum_{j=0}^{3}\mathrm{e}\left(\frac{2akj2^{\alpha-2}}{2^\alpha}\right)\\
&= \sum_{k=0}^{2^{\alpha-2}-1}\mathrm{e}\left(\frac{ak^2}{2^\alpha}\right)\sum_{j=0}^{3}\mathrm{e}\left(\frac{akj}{2}\right) = 4\sum_{k=0}^{2^{\alpha-3}-1}\mathrm{e}\left(\frac{a(2k)^2}{2^\alpha}\right)\\
&= 2\sum_{k=0}^{2^{\alpha-3}-1}\mathrm{e}\left(\frac{ak^2}{2^{\alpha-2}}\right)\sum_{j=0}^{1}\underbrace{\mathrm{e}\left(\frac{2akj2^{\alpha-3}+aj^2 2^{2\alpha-6}}{2^{\alpha-2}}\right)}_{=1}\\
&= 2\sum_{k=0}^{2^{\alpha-3}-1}\sum_{j=0}^{1}\mathrm{e}\left(\frac{a(k+2^{\alpha-3}j)^2}{2^{\alpha-2}}\right) = 2\,\mathrm{G}(a,0;2^{\alpha-2}).
\end{aligned}$$

The rest of this lemma is obtained by an easy computation. □

For the next lemma, we denote the Legendre Symbol of $a \bmod p$ by $\left(\frac{a}{p}\right)$. This factor occurs when we relate $\mathrm{G}(a,0;p)$ to $\mathrm{G}(1,0;p)$.

**Lemma 3.4.7.** *Let $p$ be an odd prime. Then*

$$\mathrm{G}(a,0;p) = \left(\frac{a}{p}\right)\mathrm{G}(1,0;p).$$

*Proof.* We know that the number of solutions of $ak^2 \equiv n \bmod p$ is $1 + \left(\frac{an}{p}\right)$. Therefore,

$$\begin{aligned}\mathrm{G}(a,0;p) &= \sum_{k=0}^{p-1} \mathrm{e}\left(\frac{ak^2}{p}\right) = \sum_{n=0}^{p-1} \mathrm{e}\left(\frac{n}{p}\right)\left(1+\left(\frac{an}{p}\right)\right) = \sum_{n=0}^{p-1} \mathrm{e}\left(\frac{n}{p}\right)\left(\frac{a}{p}\right)\left(\frac{n}{p}\right) \\ &= \left(\frac{a}{p}\right)\sum_{n=0}^{p-1} \mathrm{e}\left(\frac{n}{p}\right)\left(\frac{n}{p}\right) = \left(\frac{a}{p}\right)\mathrm{G}(1,0;p).\end{aligned}$$

□

It remains to consider the case $p = 2$.

**Lemma 3.4.8.** *Let $b$ be odd. Then $\mathrm{G}(a,b;2) = 2$ and $\mathrm{G}(a,b;2^\alpha) = 0$ for $\alpha \geq 2$.*

*Proof.* $\mathrm{G}(a,b;2) = 2$ is trivial. For the second assertion, we observe that

$$\begin{aligned}\mathrm{G}(a,b;2^\alpha) &= \sum_{j=0}^{1}\sum_{k=0}^{2^{\alpha-1}} \mathrm{e}\left(\frac{a(j2^{\alpha-1}+k)^2 + b(j2^{\alpha-1}+k)}{2^r}\right) \\ &= \sum_{k=0}^{2^{\alpha-1}} \mathrm{e}\left(\frac{ak^2+bk}{2^\alpha}\right)\sum_{j=0}^{1} \mathrm{e}\left(\frac{bj}{2}\right).\end{aligned}$$

Since $l$ is odd, the inner sum is 0. □

To complete the proof of Theorem 3.4.1 one has to compute $\mathrm{G}(1,0,m)$.

**Lemma 3.4.9.** *For any positive $m$,*

$$\mathrm{G}(1,0;m) = \frac{1}{2}(1+i^{-m})(1+i)\sqrt{m}.$$

*Proof.* We consider the Fourier series of the function $f(x) = \sum_{d=0}^{m-1} \mathrm{e}\left(\frac{(d+x)^2}{m}\right)$ with $f(0) = \mathrm{G}(1,0;m)$. Evaluating this Fourier series at $x = 0$ gives

$$\sum_{d=0}^{m-1} \mathrm{e}\left(\frac{d^2}{m}\right) = \sum_{\nu=-\infty}^{\infty} \int_0^m \mathrm{e}\left(\nu x + \frac{x^2}{m}\right) dx.$$

By changes of variables, we find a different representation:

$$\ldots = m\sum_{\nu=-\infty}^{\infty} \int_0^1 \mathrm{e}\left(m(x^2+\nu x)\right) dx = m\sum_{\nu=-\infty}^{\infty} \mathrm{e}\left(-\frac{m\nu^2}{4}\right)\int_{\nu/2}^{\nu/2+1} \mathrm{e}(my^2)dy.$$

Breaking this sum into odd and even $\nu$ yields

$$\ldots = m(1+i^{-m})\int_{-\infty}^{\infty} \mathrm{e}(my^2)dy.$$

By another change of variable, we find that

$$\ldots = (1+i^{-m})2\sqrt{m}\int_0^\infty \mathrm{e}(y^2)dy.$$

We will just sketch how to evaluate this remaining integral. We consider the integral over the path $C$ which goes along the straight line from 0 to $x \in \mathbb{R}_+$ along the circular arc from $x$ to $x\,\mathrm{e}(1/8)$ and along a straight line back to 0. Since the integrand is entire we find that the integral over the path $C$ equals 0. The integral over the arc is $\ll \frac{1}{x}$. The integral over the straight line from $x\,\mathrm{e}(1/8)$ to 0 tends to $-\mathrm{e}(1/8)\frac{1}{2\sqrt{2}}$ as $x$ tends to infinity (with an error term $\ll 1/x$). This completes this proof. □

Now we can prove Theorem 3.4.1.

*Proof of Theorem 3.4.1.* We denote by $d = \gcd(a,m)$ and find, using the lemmas above, that

$$|\mathrm{G}(a,b;m)| \le d\left|\mathrm{G}(\underbrace{a/d}_{a'},\underbrace{b/d}_{b'};\underbrace{m/d}_{m'})\right|$$

and thus by assuming that $m' = p_0^{\alpha_0}\cdots p_r^{\alpha_r}$ with $p_0 = 2$ and $\alpha_k \ge 1$ for $k \ge 1$ we find that

$$\ldots \le d\prod_{k=0}^{r}\left|\mathrm{G}\left(\underbrace{a'\frac{m'}{p_k^{\alpha_k}}}_{a_k},b';p_k^{\alpha_k}\right)\right| \le d\left|\mathrm{G}(a_0,b;2^{\alpha_0})\prod_{k=1}^{r}\mathrm{G}\left(a_k,b';p_k^{\alpha_k}\right)\right|.$$

We have also seen that for odd $b'$,

$$\left|\mathrm{G}(a,b';2^\alpha)\right| \le 1 + \mathbf{1}_{\alpha=1} \le \sqrt{22^\alpha}.$$

We also concluded, that for even $b'$

$$\left|\mathrm{G}(a,b';2^\alpha)\right| = |\mathrm{G}(a,0;2^\alpha)| \le \sqrt{2^{\alpha+1}}.$$

Thus we observe

$$\begin{aligned}
|\mathrm{G}(a,b;m)| &\le d\sqrt{22^\alpha}\prod_{k=1}^{r}\left|\mathrm{G}(a_k,b';p_k^{\alpha_k})\right| = d\sqrt{22^\alpha}\prod_{k=1}^{r}\left|\mathrm{G}(a_k,0;p_k^{\alpha_k})\right| \\
&= d\sqrt{22^\alpha}\prod_{\substack{1\le k\le r\\ 2\mid\alpha_k}}\sqrt{p_k^{\alpha_k}}\prod_{\substack{1\le k\le r\\ 2\nmid\alpha_k}}\sqrt{p_k^{\alpha_k-1}}\,|\mathrm{G}(a_k,0;p_k)| \\
&= d\sqrt{22^\alpha}\prod_{\substack{1\le k\le r\\ 2\mid\alpha_k}}\sqrt{p_k^{\alpha_k}}\prod_{\substack{1\le k\le r\\ 2\nmid\alpha_k}}\sqrt{p_k^{\alpha_k-1}}\,|\mathrm{G}(1,0;p_k)| \\
&= d\sqrt{22^\alpha}\prod_{\substack{1\le k\le r\\ 2\mid\alpha_k}}\sqrt{p_k^{\alpha_k}}\prod_{\substack{1\le k\le r\\ 2\nmid\alpha_k}}\sqrt{p_k^{\alpha_k-1}}\sqrt{p_k} \\
&= d\sqrt{2\prod_{k=0}^{r}p_k^{\alpha_k}} = \sqrt{2(m'd)d} = \sqrt{2md}.
\end{aligned}$$

□

Consequently we obtain the following result for incomplete quadratic Gauss sums.

**Lemma 3.4.10.** *For all $(a, b, m, N, n_0) \in \mathbb{Z}^5$ with $m \geq 1$ and $N \geq 0$, we have*

$$\left| \sum_{n=n_0+1}^{n_0+N} \mathrm{e}\left(\tfrac{an^2+bn}{m}\right) \right| \leq \left(\tfrac{N}{m} + 1 + \tfrac{2}{\pi} \log \tfrac{2m}{\pi}\right) \sqrt{2m \gcd(a, m)}. \tag{3.19}$$

*Proof.* The following argument is a variant of a method known at least since Vinogradov.

For $m = 1$ the result is true; thus we assume that $m \geq 2$. There are $\lfloor N/m \rfloor$ complete sums whose absolute values are bounded from above by $\sqrt{2m \gcd(a, m)}$. The remaining sum is either empty or of the form

$$S = \sum_{n=n_1+1}^{n_1+L} \mathrm{e}\left(\tfrac{an^2+bn}{m}\right)$$

for some $n_1 \in \mathbb{Z}$ and $1 \leq L \leq m$. Therefore we see that,

$$\begin{aligned} S &= \sum_{u=n_1+1}^{n_1+L} \sum_{n=0}^{m-1} \mathrm{e}\left(\tfrac{an^2+bn}{m}\right) \frac{1}{m} \sum_{k=0}^{m-1} \mathrm{e}\left(k\tfrac{n-u}{m}\right) \\ &= \frac{1}{m} \sum_{k=0}^{m-1} \sum_{u=n_1+1}^{n_1+L} \mathrm{e}\left(\tfrac{-ku}{m}\right) \sum_{n=0}^{m-1} \mathrm{e}\left(\tfrac{an^2+(b+k)n}{m}\right), \end{aligned}$$

and thus

$$S \leq \frac{1}{m} \sum_{k=0}^{m-1} \min\left(L, \left|\sin \tfrac{\pi k}{m}\right|^{-1}\right) \left| \sum_{n=0}^{m-1} \mathrm{e}\left(\tfrac{an^2+(b+k)n}{m}\right) \right|.$$

We observe, by convexity of $t \mapsto 1/\sin(\pi t/m)$, that,

$$\frac{1}{m} \sum_{k=0}^{m-1} \min\left(L, \left|\sin \tfrac{\pi k}{m}\right|^{-1}\right) \leq 1 + \frac{1}{m} \int_{1/2}^{m-1/2} \frac{dt}{\sin \frac{\pi t}{m}} = 1 + \frac{2}{\pi} \log \cot \frac{\pi}{2m}.$$

Applying Theorem 3.4.1 with $b$ replaced by $b + k$ we obtain (3.19). □

## 3.5 Carry Lemmas

As mentioned before, we want to find a quantitative statement on how rare carry propagation along several digits is.

**Lemma 3.5.1.** *Let $(\nu, \lambda, \rho) \in \mathbb{N}^3$ such that $\nu + \rho \leq \lambda \leq 2\nu$. For any integer $r$ with $0 \leq r \leq q^\rho$, the number of integers $n < q^\nu$ for which there exists an integer $j \geq \lambda$ with $\varepsilon_j((n+r)^2) \neq \varepsilon_j(n^2)$ is $\ll q^{2\nu+\rho-\lambda}$. Hence, the number of integers $n < q^\nu$ with*

$$\mathrm{s}_\lambda((n+r)^2) - \mathrm{s}_\lambda(n^2) \neq \mathrm{s}((n+r)^2) - \mathrm{s}(n^2)$$

*is also $\ll q^{2\nu+\rho-\lambda}$.*

*Proof.* We follow the idea of [17] with some minor changes to suit our case better.

First we suppose that $\lambda \geq \nu + \rho + 3$; otherwise we know that the number of all integers $n < q^\nu$ is bounded by $q^\nu \leq q^{\nu-\lambda+\nu+\rho+2} = q^2 \cdot q^{2\nu+\rho-\lambda}$.

We know that $2nr+r^2 < 2q^{\rho+\nu}+q^{2\rho} \leq 3q^{\rho+\nu} < q^{\rho+\nu+2}$. In order to affect the $j$-th digit for $j \geq \lambda$, it is necessary to transfer a carry for the digits $\rho+\nu+2$ to $j$. Therefore, for $\rho+\nu+2 \leq j' < \lambda$, $a_{j'} = q-1$ must hold. Hence there exists $m \in \mathbb{N}$ such that $\lfloor n^2/q^{\rho+\nu+2} \rfloor = q^{\lambda-\nu-\rho-2}m - 1$. In other words:

$$q^{\lambda-\nu-\rho-2}m - 1 \leq \frac{n^2}{q^{\nu+\rho+2}} < q^{\lambda-\nu-\rho-2}m.$$

Therefore, we can bound $m \in \mathbb{N}$

$$\frac{n^2}{q^\lambda} < m \leq \left\lfloor \frac{q^{2\nu}}{q^\lambda} + \frac{1}{q^{\lambda-\nu-\rho-2}} \right\rfloor = q^{2\nu-\lambda}.$$

For fixed $m$, there are at most $\sqrt{q^\lambda m} - \sqrt{q^\lambda m - q^{\nu+\rho+2}} = \sqrt{q^\lambda m}\left(1 - \sqrt{1 - \frac{1}{mq^{\lambda-\nu-\rho-2}}}\right)$ integers $n$ such that $\lfloor n^2/q^{\nu+\rho+2} \rfloor = q^{\lambda-\nu-\rho-2}m - 1$.

For $0 \leq u \leq 1$ it holds that $1 - \sqrt{1-u} \leq u$. Since $mq^{\lambda-\nu-\rho-2} \geq 1$, we know that the number of integers $n < q^\nu$ for which there exists an integer $j \geq \lambda$ with $\varepsilon_j((n+r)^2) \neq \varepsilon_j(n^2)$ is bounded by

$$\begin{aligned}\sum_{m=1}^{q^{2\nu-\lambda}} \sqrt{q^\lambda m}\left(1 - \sqrt{1 - \frac{1}{mq^{\lambda-\nu-\rho-2}}}\right) &\leq \sum_{m=1}^{q^{2\nu-\lambda}} \frac{\sqrt{q^\lambda m}}{q^{\lambda-\nu-\rho-2}m} = q^{\nu+\rho+2-\lambda/2} \sum_{m=1}^{q^{2\nu-\lambda}} \frac{1}{\sqrt{m}} \\ &\overset{(*)}{\leq} q^{5/2} q^{2\nu+\rho-\lambda}.\end{aligned}$$

The last inequality $(*)$ holds since

$$\begin{aligned}\sum_{m=1}^{q^n} \frac{1}{\sqrt{m}} &= q^{-\frac{n}{2}} + \sum_{\ell=1}^{n} \sum_{m=q^{\ell-1}}^{q^\ell-1} \frac{1}{\sqrt{m}} \leq 1 + \sum_{\ell=1}^{n} (q^\ell - q^{\ell-1}) \frac{1}{\sqrt{q^{\ell-1}}} \\ &\leq 1 + \sum_{\ell=1}^{n} \left(q^{\frac{\ell+1}{2}} - q^{\frac{\ell-1}{2}}\right) = 1 + q^{\frac{n+1}{2}} - 1 = q^{\frac{1}{2}} q^{\frac{n}{2}}.\end{aligned}$$

This completes the proof. □

The next lemma helps to replace quadratic exponential sums by linear exponential sums.

**Lemma 3.5.2.** *Let $(\lambda, \mu, \nu, \rho') \in \mathbb{N}^4$ such that $0 < \mu < \nu < \lambda$, $2\rho' \leq \mu \leq \nu - \rho'$ and $\lambda - \nu \leq 2(\mu - \rho')$ and set $\mu' = \mu - \rho'$. For integers $n < q^\nu$, $s \geq 1$ and $1 \leq r \leq q^{(\lambda-\nu)/2}$ we set*

$$\begin{aligned} n^2 &\equiv u_1 q^{\mu'} + w_1 \bmod q^\lambda && (0 \leq w_1 < q^{\mu'},\ 0 \leq u_1 < q^{\lambda-\mu+\rho'}) \\ (n+r)^2 &\equiv u_2 q^{\mu'} + w_2 \bmod q^\lambda && (0 \leq w_2 < q^{\mu'},\ 0 \leq u_2 < q^{\lambda-\mu+\rho'}) \\ 2n &\equiv u_3 q^{\mu'} + w_3 \bmod q^\lambda && (0 \leq w_3 < q^{\mu'},\ 0 \leq u_3 < q^{\nu+1-\mu+\rho'}) \\ 2sn &\equiv v \bmod q^{\lambda-\mu}, && (0 \leq v < q^{\lambda-\mu}) \end{aligned} \tag{3.20}$$

*where the integers* $u_1 = u_1(n)$, $u_2 = u_2(n)$ ,$u_3 = u_3(n)$, $v = v(n)$ ,$w_1 = w_1(n)$, $w_2 = w_2(n)$ *and* $w_3 = w_3(n)$ *satisfy the above conditions. Then for any integer* $\ell \geq 1$ *the number of integers* $n < q^\nu$ *for which one of the following conditions*

$$\begin{aligned} \mathrm{s}_{\mu,\lambda}((n+\ell)^2) &\neq \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1 + \ell u_3) \\ \mathrm{s}_{\mu,\lambda}((n+\ell+sq^\mu)^2)) &\neq \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1 + \ell u_3 + vq^{\rho'} + 2\ell s q^{\rho'}) \\ \mathrm{s}_{\mu,\lambda}((n+r+\ell)^2) &\neq \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_2 + \ell u_3) \\ \mathrm{s}_{\mu,\lambda}((n+r+\ell+sq^\mu)^2)) &\neq \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_2 + \ell u_3 + vq^{\rho'} + 2(\ell+r) s q^{\rho'}) \end{aligned} \tag{3.21}$$

*is satisfied is* $\ll q^{\nu-\rho'}$.

*Proof (by [7]).* We first consider the case $(n+\ell)^2$. The other cases are similar and we will comment on them at the end of the proof. We find that

$$(n+\ell)^2 = (u_1 + \ell u_3) q^{\mu'} + w_1 + \ell w_3 + \ell^2 \bmod q^\lambda.$$

If $w_1 + \ell w_3 + \ell^2 < q^{\mu'}$ and $0 \leq j < \lambda - \mu'$, we have $\varepsilon_{\mu'+j}((n+\ell)^2) = \varepsilon_j(u_1 + \ell u_3)$. For $w_1 + \ell w_3 + \ell^2 \geq q^{\mu'}$, there is a carry propagation. We show that there are only few exceptions where more than $\rho'$ digits are changed. The proof is split into the following two steps:

1. If the digits block $(\varepsilon_j((n+\ell)^2))_{\mu \leq j < \lambda}$ differ from the digits block $(\varepsilon_j(u_1 + \ell u_3))_{\rho' \leq j < \lambda - \mu + \rho'}$, where $u_1 = u_1(n)$ and $u_3 = u_3(n)$ are defined by (3.20), it follows that

$$\frac{(n+\ell)^2}{q^\mu} - \left\lfloor \frac{(n+\ell)^2}{q^\mu} \right\rfloor \leq \frac{C}{q^{\rho'}} \quad \text{or} \quad \frac{(n+\ell)^2}{q^\mu} - \left\lfloor \frac{(n+\ell)^2}{q^\mu} \right\rfloor \geq 1 - \frac{C}{q^{\rho'}}, \tag{3.22}$$

   for some constant $C = C(\ell)$.

2. The number of integers $n < q^\nu$ with (3.22) is $\ll q^{\nu-\rho'}$.

Obviously these two properties are sufficient to prove Lemma 3.5.2.

We start with the proof of the first property. As mentioned above we just have to consider the case $w_1 + \ell w_3 + \ell^2 \geq q^{\mu'} = q^{\mu-\rho'}$. Since $w_1, w_3 < q^{\mu'}$ the carry

$$\widetilde{w} := \left\lfloor q^{-\mu'} \left( w_1 + \ell w_3 + \ell^2 \right) \right\rfloor$$

is bounded and, thus, can only attain finitely many values $\{1, 2, \ldots, D\}$ (where $D$ is a constant depending on $\ell$). These values of $\widetilde{w}$ will certainly affect some digits (of lower order) of $u_1 + \ell u_3$. Let $\widetilde{v} := u_1 + \ell u_3 \bmod q^{\rho'}$ with $0 \leq \widetilde{v} < q^{\rho'}$. The digits $\varepsilon_j(u_1 + \ell u_3)$, $\rho' \leq j < \lambda - \mu'$ might be affected by this carry if $\widetilde{v} \in \{q^{\rho'} - 1, q^{\rho'} - 2, \ldots, q^{\rho'} - D\}$. Since

$$\begin{aligned} \frac{(n+\ell)^2}{q^\mu} &\equiv \frac{u_1 + \ell u_3}{q^{\rho'}} + \frac{w_1 + \ell w_3 + \ell^2}{q^{\mu'+\rho'}} \bmod 1 \\ &\equiv \frac{\widetilde{v}}{q^{\rho'}} + \frac{w_1 + \ell w_3 + \ell^2}{q^{\mu'+\rho'}} \bmod 1, \end{aligned}$$

it immediately follows that (3.22) holds with $C = D + 1$. This completes the proof of the first part.

Next, let $Z$ denote the number of integers $n < q^\nu$ with (3.22). By Lemma 3.1.1, we have

$$\begin{aligned} Z &= \sum_{n<q^\nu} \left(\chi_\alpha\left(q^{-\mu}(n+\ell)^2\right) + \chi_\alpha\left(-q^{-\mu}(n+\ell)^2\right)\right) \\ &\le 2\sum_{|h|\le H}\left(\alpha+\frac{1}{H}\right)\left|\sum_{n<q^\nu} \mathrm{e}\left(h\frac{(n+\ell)^2}{q^\mu}\right)\right| \end{aligned}$$

with $\alpha = Cq^{-\rho'}$. We can set $H = q^{\rho'}$.

It is clear that the main contribution comes from the term corresponding to $h = 0$ which gives an upper bound of form $\mathcal{O}(q^{\nu-\rho'})$. Each $h \neq 0$ with $|h| \le H = q^{\rho'}$ can be written as $h = h'd$, where $d \mid q^\mu$ and $\gcd(h', q) = 1$. Therefore, we have by Lemma 3.4.10

$$\sum_{n<q^\nu} \mathrm{e}\left(h\frac{(n+\ell)^2}{q^\mu}\right) = \mathcal{O}\left(q^{\nu-\mu/2}\sqrt{d} + \mu q^{\mu/2}\sqrt{d}\right)$$

and, consequently,

$$q^{-\rho'}\sum_{0\neq|h|\le q^{\rho'}}\left|\sum_{n<q^\nu} \mathrm{e}\left(h\frac{(n+\ell)^2}{q^\mu}\right)\right| = \mathcal{O}\left((q^{-\rho'}q^{\nu-\mu/2} + \mu q^{\mu/2})\sum_{\substack{d\mid q^\mu \\ d\le q^{\rho'}}}\frac{q^{\rho'}}{d}\sqrt{d}\right).$$

This equals $\mathcal{O}\left(q^{\nu-\mu/2} + \mu q^\mu\right)$ since

$$\sum_{d\mid q^\mu} d^{-1/2} \le \prod_{j=1}^{\omega(q)} \frac{1}{1-\frac{1}{\sqrt{p_j}}}.$$

where $p_1, \ldots, p_{\omega(q)}$ are exactly the prime divisors of $q$. Since $2\rho' \le \mu \le \nu - \rho'$, all contributions are $\ll q^{\nu-\rho'}$. This completes the proof of the second part.

Finally, we comment on the other cases. First, there is no change for $(n+\ell+sq^\mu)^2$ since the term $sq^\mu$ does not affect the discussed carry propagation. For $(n+\ell+r)^2$, we have

$$(n+\ell+r)^2 = (u_2+\ell u_3)q^{\mu'} + w_2 + \ell w_3 + \ell^2 + 2r\ell.$$

Here we have to assure that $q^{-\mu'}(w_2 + \ell w_3 + \ell^2 + 2r\ell)$ remains bounded. However, this is ensured by the assumption $\lambda - \nu \le 2(\mu - \rho')$. The same argument applies for the final case $(n+\ell+sq^\mu+r)^2$. □

# 4 Proof of the Main Theorem

In this chapter, we complete the proof of Theorem 1.2.2 following the ideas and structure of [7]. We use Proposition 2.2.3 for the cases $K \equiv 0 \bmod 1$ and Proposition 2.2.4 for the case $K \not\equiv 0 \bmod 1$.

The structure of the proof is similar for both cases: At first we want to substitute the function $s$ by $\mathrm{s}_{\mu,\lambda}$. This can be done by applying Lemma 3.5.1 and Lemma 3.2.1 in the case $K \equiv 0 \bmod 1$. For the case $K \not\equiv 0 \bmod 1$ we have to use Lemma 3.2.1 first.

Thereafter, we apply Lemma 3.5.2 to reduce the quadratic terms to linear ones. Next, we use characteristic functions to detect suitable values for $u_1(n), u_2(n), u_3(n)$. Lemma 3.1.8 allows us to replace the characteristic functions by exponential sums. We split the remaining exponential sum into a quadratic and a linear part and find that the quadratic part is negligibly small. For the remaining sum, we need Proposition 2.2.3 or 2.2.4 – depending on the value of $K \bmod 1$. The case $K \not\equiv 0 \bmod 1$ needs more effort to deal with.

## 4.1 The case $K \equiv 0 \bmod 1$

In this section, we show that, if $K = \alpha_0 + \cdots + \alpha_{k-1} \equiv 0 \bmod 1$, Proposition 2.2.3 provides an upper bound for the sum

$$S_0 = \sum_{n<N} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell \, \mathrm{s}((n+\ell)^2)\right).$$

Let $\nu$ be the unique integer such that $q^{\nu-1} < N \le q^\nu$ and $(\lambda, \mu) \in \mathbb{N}^2$ such that

$$\mu < \nu < \lambda \text{ and } \lambda - \nu = \nu - \mu = \tfrac{1}{2}(\lambda - \mu). \tag{4.1}$$

The precise values will be specified later.

We will choose all occurring exponents, e.g. $\mu, \lambda$, as fractions of $\nu$. Therefore we are not concerned about sums of form, $\mathcal{O}(q^{2\nu-\lambda}) = \mathcal{O}(N^{1-\eta'})$, for example.

By using Lemma 3.5.1, it follows that the number of integers $n < N$ such that the $j$-th digits of $n^2$, $(n+1)^2$, …, $(n+k-1)^2$ coincide for $j \ge \lambda$ is equal to $N - \mathcal{O}(Nq^{-(\lambda-\nu)})$. Furthermore, since $K \equiv 0 \bmod 1$ it follows that we obtain for those $n$

$$\sum_{\ell=0}^{k-1} \alpha_\ell \, \mathrm{s}_{\lambda,\infty}((n+\ell)^2) = K \, \mathrm{s}_{\lambda,\infty}(n^2) \in \mathbb{Z}, \text{ where } \mathrm{s}_{\lambda,\infty} = \mathrm{s} - \mathrm{s}_\lambda \,.$$

Consequently, if we set

$$S_1 = \sum_{n<N} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell \, \mathrm{s}_\lambda((n+\ell)^2)\right),$$

the summands of $S_0$ and $S_1$ coincide except for at most $\mathcal{O}(Nq^{-(\lambda-\nu)})$ and thus

$$S_0 = S_1 + \mathcal{O}\left(q^{\nu-(\lambda-\nu)}\right). \tag{4.2}$$

Now we use Lemma 3.2.1 to substitute $\mathrm{s}_\lambda$ by $\mathrm{s}_{\mu,\lambda}$.

By applying Lemma 3.2.1 with $Q = q^\mu$ and $S = q^{\nu-\mu}$ we obtain

$$|S_1|^2 \ll \frac{N^2}{S} + \frac{N}{S}\Re(S_2), \tag{4.3}$$

with

$$S_2 = \sum_{1\le s<S}\left(1-\frac{s}{S}\right)S_2'(s)$$

and

$$S_2'(s) = \sum_{n\in I(N,s)} \mathrm{e}\left(\sum_{\ell=0}^{k-1}\alpha_\ell(\mathrm{s}_{\mu,\lambda}((n+\ell)^2) - \mathrm{s}_{\mu,\lambda}((n+\ell+sq^\mu)^2))\right),$$

where $I(N,s)$ is an interval included in $[0,N-1]$ (which we do not specify).

Since $\frac{N^2}{S} = \mathcal{O}(q^{\nu-\mu/2})$ is negligible, we are just concerned about $\frac{N}{S}\Re(S_2)$.

The right-hand side of $S_2'(s)$ depends only on the digits of $(n+\ell)^2$ and $(n+\ell+sq^\mu)^2$ between $\mu$ and $\lambda$. Next we use Lemma 3.5.2 to reduce these quadratic terms to linear terms with a negligible error term. Therefore, we have to take the digits between $\mu' = \mu-\rho'$ and $\mu$ into account, where $\rho' > 0$ will be chosen in a proper way (as a fraction of $\nu$). We set the integers $u_1 = u_1(n)$, $u_3 = u_3(n)$, $v = v(n)$, $w_1 = w_1(n)$, and $w_3 = w_3(n)$ to satisfy the conditions of Lemma 3.5.2:

$$\begin{aligned}
n^2 &\equiv u_1 q^{\mu'} + w_1 \bmod q^\lambda && (0\le w_1 < q^{\mu'},\ 0\le u_1 < U_1 = q^{\lambda-\mu'})\\
2n &= u_3 q^{\mu'} + w_3 && (0\le w_3 < q^{\mu'},\ 0\le u_3 < U_3 = q^{\nu-\mu'+1})\\
2sn &\equiv v \bmod q^{\lambda-\mu} && (0\le v < q^{\lambda-\mu}).
\end{aligned}$$

By assuming that

$$2\mu' \ge \lambda, \tag{4.4}$$

we have

$$\begin{aligned}
(n+\ell)^2 &\equiv (u_1+\ell u_3)q^{\mu'} + w_1 + \ell w_3 + \ell^2 \bmod q^\lambda,\\
(n+\ell+sq^\mu)^2 &\equiv (u_1+\ell u_3 + vq^{\rho'} + \ell 2sq^{\rho'})q^{\mu'} + w_1 + \ell w_3 + \ell^2 \bmod q^\lambda.
\end{aligned}$$

By Lemma 3.5.2, it follows that

$$\begin{aligned}
\mathrm{s}_{\mu,\lambda}((n+\ell)^2) &= \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3),\\
\mathrm{s}_{\mu,\lambda}((n+\ell+sq^\mu)^2)) &= \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3 + vq^{\rho'} + 2\ell sq^{\rho'})
\end{aligned}$$

for any integer $n < N$ with at most $\mathcal{O}(q^{\nu-\rho'})$ exceptions. Hence it suffices to consider the sum

$$S_3'(s) = \sum_{n\in I(N,s)} \mathrm{e}\left(\sum_{\ell=0}^{k-1}\alpha_\ell(\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3) - \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3 + vq^{\rho'} + 2\ell sq^{\rho'})\right)$$

- where $u_1 = u_1(n), u_3 = u_3(n), v = v(n)$ - since there again holds

$$S_2'(s) = S_3'(s) + \mathcal{O}(q^{\nu-\rho'}). \tag{4.5}$$

Next, we implement our definitions of $u_1(n), u_3(n)$ by using characteristic functions. We define $S_3'(s)$ as

$$\begin{aligned} S_3'(s) = \sum_{0\le u_1<U_1} \sum_{0\le u_3<U_3} \sum_{n\in I(N,s)} \\ \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell(\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3) - \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+v(n)q^{\rho'}+2\ell s q^{\rho'})\right) \\ \chi_{q^{\mu'-\lambda}}\left(\frac{n^2}{q^\lambda} - \frac{u_1}{U_1}\right) \chi_{q^{\mu'-\nu-1}}\left(\frac{2n}{q^{\nu+1}} - \frac{u_3}{U_3}\right), \end{aligned}$$

where $\chi_\alpha$ is defined by (3.1). Lemma 3.1.8 allows us to replace the product of characteristic functions $\chi$ by a product of trigonometric polynomials. More precisely, using (3.11) with $H_1 = U_1 q^{\rho''}$ and $H_3 = U_3 q^{\rho''}$ for some suitable $\rho'' > 0$ (which is chosen later and again as a fraction of $\nu$), we have

$$S_3'(s) = S_4(s) + \mathcal{O}(E_1) + \mathcal{O}(E_3) + \mathcal{O}(E_{1,3}), \tag{4.6}$$

where $E_1, E_3$ and $E_{1,3}$ are the error terms specified in (3.11) and

$$\begin{aligned} S_4(s) \;=\; & \sum_{0\le u_1<U_1} \sum_{0\le u_3<U_3} \sum_{0\le v<q^{\lambda-\mu}} \\ & \sum_{n\in I(N,s)} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell(\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3) - \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+vq^{\rho'}+2\ell s q^{\rho'}))\right) \\ & A_{U_1^{-1},H_1}\left(\frac{n^2}{q^\lambda} - \frac{u_1}{U_1}\right) A_{U_3^{-1},H_3}\left(\frac{2n}{q^{\nu+1}} - \frac{u_3}{U_3}\right) \frac{1}{q^{\lambda-\mu}} \sum_{0\le h<q^{\lambda-\mu}} \mathrm{e}\left(h\frac{2sn-v}{q^{\lambda-\mu}}\right), \end{aligned}$$

the inner most sum *filters* the correct value of $v = v(n)$.

The error terms $E_1$, $E_3$, $E_{1,3}$ can easily be estimated with the help of Lemma 3.4.10:

$$E_1 = \frac{1}{q^{\rho''}} \sum_{|\overline{h}_1|\le q^{\rho''}} \left|\sum_n \mathrm{e}\left(\frac{\overline{h}_1 n^2}{q^{\mu'}}\right)\right| \ll q^{\nu-\rho''} + \rho'' q^{\nu-\mu'/2} \ll q^{\nu-\rho''},$$

$$E_3 = \frac{1}{q^{\rho''}} \sum_{|\overline{h}_3|\le q^{\rho''}} \left|\sum_n \mathrm{e}\left(\frac{\overline{h}_3 2n}{q^{\mu'}}\right)\right| \ll q^{\nu-\rho''} + \rho'' q^{\nu-\mu'} \ll q^{\nu-\rho''},$$

$$E_{1,3} = \frac{1}{q^{2\rho''}} \sum_{|\overline{h}_1|\le q^{\rho''}} \sum_{|\overline{h}_3|\le q^{\rho''}} \left|\sum_n \mathrm{e}\left(\frac{\overline{h}_1 n^2}{q^{\mu'}} + \frac{\overline{h}_3 2n}{q^{\mu'}}\right)\right| \ll q^{\nu-\rho''},$$

provided that

$$\rho'' < \mu'/2 \text{ and } \mu' \ll q^{\nu-\mu'}. \tag{4.7}$$

Therefore, the error terms $E_1$, $E_3$, and $E_{1,3}$ are negligible (since $\rho'' \to \infty$) and so we just have to concentrate on $S_4(s)$. By using the representations of $A_{U_1^{-1},H_1}$ and $A_{U_3^{-1},H_3}$, we obtain

$$\begin{aligned} S_4(s) =& \frac{1}{q^{\lambda-\mu}} \sum_{|h_1|\le H_1} \sum_{|h_3|\le H_3} \sum_{0\le h<q^{\lambda-\mu}} a_{h_1}(U_1^{-1},H_1)\, a_{h_3}(U_3^{-1},H_3) \\ & \sum_{0\le u_1<U_1} \sum_{0\le u_3<U_3} \sum_{0\le v<q^{\lambda-\mu}} \mathrm{e}\left(-\frac{h_1u_1}{U_1}-\frac{h_3u_3}{U_3}-\frac{hv}{q^{\lambda-\mu}}\right) \\ & \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell(\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3)-\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+v2^{\rho'}+2\ell s q^{\rho'}))\right) \\ & \cdot \sum_n \mathrm{e}\left(\frac{h_1n^2}{q^\lambda}+\frac{h_3n}{q^\nu}+\frac{2hsn}{q^{\lambda-\mu}}\right), \end{aligned}$$

where by (3.4),

$$|a_{h_1}(U_1^{-1},H_1)| \le U_1^{-1} \quad \text{and} \quad |a_{h_3}(U_3^{-1},H_3)| \le U_3^{-1}. \tag{4.8}$$

The first step in the analysis of $S_4(s)$ is to observe that we only have to take the term that corresponds to $h_1 = 0$ into account. For $h_1 \neq 0$, we can estimate the exponential sum in the following way: By Lemma 3.4.10 we have

$$\sum_n \mathrm{e}\left(\frac{h_1n^2}{q^\lambda}+\frac{h_3n}{q^\nu}+\frac{2hsn}{q^{\lambda-\mu}}\right) \ll \left(Nq^{-\lambda}+1+\lambda\right)\sqrt{q^\lambda \gcd(h_1,q^\lambda)} \ll \lambda q^{\lambda/2}\sqrt{\gcd(h_1,q^\lambda)}.$$

Furthermore we find

$$\sum_{1\le h_1\le H_1} \sqrt{\gcd(h_1,q^\lambda)} \le \sum_{d\mid q^\lambda} \sqrt{d} \sum_{1\le \overline{h_1}\le H_1/d} 1 = \sum_{d\mid q^\lambda} \sqrt{d}\frac{H_1}{d} = H_1 \sum_{d\mid q^\lambda} \frac{1}{\sqrt{d}}. \tag{4.9}$$

Let $q = p_1^{e_1}\cdots p_{\omega(q)}^{e_{\omega(q)}}$ be the prime decomposition of $q$. Then

$$\begin{aligned} \sum_{d\mid q^\lambda} \frac{1}{\sqrt{d}} &= \sum_{e_1'\le e_1\lambda} \cdots \sum_{e_{\omega(q)}'\le e_{\omega(q)}\lambda} p_1^{-e_1'/2}\cdots p_{\omega(q)}^{-e_{\omega(q)}'/2} \\ &\le \left(\sum_{e_1'=0}^{\infty}\left(\frac{1}{\sqrt{p_1}}\right)^{e_1'}\right)\cdots\left(\sum_{e_{\omega(q)}'=0}^{\infty}\left(\frac{1}{\sqrt{p_{\omega(q)}}}\right)^{e_{\omega(q)}'}\right) = \prod_{j=1}^{\omega(q)} \frac{1}{1-\frac{1}{\sqrt{p_j}}}, \end{aligned}$$

is constant since we fixed $q$. In conclusion, by using $|\mathrm{e}(x)| = 1$ and (4.8), we can bound the absolute value of the contribution of $h_1 \neq 0$ by

$$\sum_{0<|h_1|\le H_1} \sum_{|h_3|\le H_3} \sum_{0\le h<q^{\lambda-\mu}} \left|\sum_n \mathrm{e}\left(\frac{h_1n^2}{q^\lambda}+\frac{h_3n}{q^\nu}+\frac{2hsn}{q^{\lambda-\mu}}\right)\right| \ll \lambda H_1H_3q^{\lambda/2+\lambda-\mu}.$$

We assume that

$$(\nu-\mu)+2(\lambda-\mu)+2(\rho'+\rho'') \le \lambda/4 \tag{4.10}$$

(which will be justified later) so that

$$S_4(s) = S_5(s) + \mathcal{O}(\lambda q^{3\lambda/4}), \tag{4.11}$$

where $S_5(s)$ denotes the part of $S_4(s)$ with $h_1 = 0$.

By applying the triangle inequality and by estimating the remaining exponential sum by (3.13), we obtain

$$|S_5(s)| \le \frac{1}{U_1 U_3 q^{\lambda-\mu}} \sum_{|h_3|\le H_3} \sum_{0\le h<q^{\lambda-\mu}} \sum_{0\le u_3<U_3} \left| \sum_{0\le u_1<U_1} \sum_{0\le v<q^{\lambda-\mu}} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell(\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3) - \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+vq^{\rho'}+2\ell s q^{\rho'})) - \frac{hv}{q^{\lambda-\mu}}\right)\right| \cdot \min\left(N, \left|\sin\left(\pi\left(\frac{h_3}{q^\nu}+\frac{2hs}{q^{\lambda-\mu}}\right)\right)\right|^{-1}\right).$$

By setting $u_1 = u_1'' + q^{\rho'}u_1'$ and $u_3 = u_3'' + q^{\rho'}u_3'$ (where $0 \le u_1'', u_3'' < q^{\rho'}$) we get

$$\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3) = \mathrm{s}_{\lambda-\mu}(u_1'+\ell u_3'+i_\ell),$$
$$\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+vq^{\rho'}+2\ell s q^{\rho'}) = \mathrm{s}_{\lambda-\mu}(u_1'+v+\ell(u_3'+2s)+i_\ell)$$

with $i_\ell = \lfloor (u_1''+\ell u_3'')/q^{\rho'} \rfloor$. As $I = (i_\ell)_{0\le\ell<k} = (\lfloor (u_1''+\ell u_3'')/q^{\rho'}\rfloor)_{0\le\ell<k}$ is contained in $\mathcal{I}_k$, we have

$$S_5(s) \le \frac{1}{q^{2(\lambda-\mu)+(\nu-\mu+1)}} \sum_{|h_3|\le H_3} \sum_{0\le h<q^{\lambda-\mu}} \sum_{0\le u_3'<q^{\nu-\mu+1}} \max_{I\in\mathcal{I}_k} \left| \sum_{0\le u_1'<q^{\lambda-\mu}} \sum_{0\le v<q^{\lambda-\mu}} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell(\mathrm{s}_{\lambda-\mu}(u_1'+\ell u_3'+i_\ell) - \mathrm{s}_{\lambda-\mu}(u_1'+v+\ell(u_3'+2s)+i_\ell) - \frac{hv}{q^{\lambda-\mu}}\right)\right| \cdot \min\left(N, \left|\sin\left(\pi\left(\frac{h_3}{q^\nu}+\frac{2hs}{q^{\lambda-\mu}}\right)\right)\right|^{-1}\right).$$

By substituting $u_1' + v$ by another variable $\overline{u}_1'$, using the definition of $G^I_{\lambda-\mu}(h,d)$ and replacing the maximum by a sum we obtain

$$S_5(s) \le \sum_{|h_3|\le H_3} \sum_{0\le h<q^{\lambda-\mu}} \frac{1}{q^{\nu+1-\mu}} \sum_{0\le u_3'<q^{\nu-\mu+1}} \sum_{I\in\mathcal{I}_k} \left|G^I_{\lambda-\mu}(h,u_3')\overline{G^I_{\lambda-\mu}(h,u_3'+2s)}\right| \cdot \min\left(N, \left|\sin\left(\pi\left(\frac{h_3}{q^\nu}+\frac{2hs}{q^{\lambda-\mu}}\right)\right)\right|^{-1}\right).$$

Using the estimate $\left|G^I_{\lambda-\mu}(h,u_3'+2s)\right| \le 1$ and the Cauchy-Schwarz inequality, we yield

$$\sum_{0\le u_3'<q^{\nu-\mu+1}} \left|G^I_{\lambda-\mu}(h,u_3')\overline{G^I_{\lambda-\mu}(h,u_3'+2s)}\right| \le q^{(\nu-\mu+1)/2} \left(\sum_{0\le u_3'<q^{\nu-\mu+1}} \left|G^I_{\lambda-\mu}(h,u_3')\right|^2\right)^{1/2}.$$

We now replace $\lambda$ by $\lambda-\mu$, $\lambda'$ by $\nu-\mu+1$ and use (4.1) and apply Proposition 2.2.3.

$$S_5(s) \ll q^{-\eta(\lambda-\mu)/2} \sum_{|h_3|\le H_3} \sum_{0\le h<q^{\lambda-\mu}} \min\left(N, \left|\sin\left(\pi\left(\frac{h_3}{q^\nu}+\frac{2hs}{q^{\lambda-\mu}}\right)\right)\right|^{-1}\right).$$

We now take the dependency on $s$ into account and average according to it. Since $|h_3|/q^\nu \le 1/2$, we obtain from (3.16) that

$$\begin{aligned}\frac{1}{S}\sum_{1\le s\le S}\sum_{0\le h<q^{\lambda-\mu}} \min\left(q^\nu, \left|\sin\left(\pi\left(\frac{h_3}{q^\nu}+\frac{2hs}{q^{\lambda-\mu}}\right)\right)\right|^{-1}\right)\\ \ll (\lambda-\mu)^{\omega(q)}\min\left(q^\nu, \left|\sin\left(\pi\frac{h_3}{q^\nu}\right)\right|^{-1}\right)+(\lambda-\mu)q^{\lambda-\mu}\end{aligned}$$

Finally, we have

$$\sum_{|h_3|\le H_3}\min\left(q^\nu, \left|\sin\left(\pi\frac{h_3}{q^\nu}\right)\right|^{-1}\right) \ll \nu\, q^\nu$$

and thus we obtain the estimate

$$\begin{aligned}\frac{1}{S}\sum_{1\le s\le S}|S_5(s)| &\le q^{-\eta(\lambda-\mu)/2}\nu^{\omega(q)+1}q^\nu + q^{-\eta(\lambda-\mu)/2}H_3(\lambda-\mu)q^{\lambda-\mu}\\ &\ll q^{-\eta(\lambda-\mu)/2}\nu^{\omega(q)+1}q^\nu\end{aligned}$$

provided that

$$\nu-\mu'+\rho''+\lambda-\mu\le\nu. \tag{4.12}$$

Putting all these estimates – (4.2), (4.3), (4.5), (4.6) and (4.11) – together and recalling that $\mu'=\mu-\rho'$, we finally find the upper bound

$$|S_0| \ll q^{\nu-(\lambda-\nu)} + \nu^{(\omega(q)+1)/2}q^\nu q^{-\eta(\lambda-\nu)/2} + q^{\nu-\rho'/2} + q^{\nu-\rho''/2} + \lambda^{1/2}q^{\nu/2+3\lambda/8}$$

– provided that the conditions (4.1) (4.4), (4.7), (4.10), (4.12) hold, i.e.

$$\begin{aligned}&2\rho'\le\mu\le\nu-\rho', \quad \rho''<\mu'/2, \quad \mu'\ll 2^{\nu-\mu'}, \quad 2\mu'\ge\lambda,\\ &(\nu-\mu)+2(\lambda-\mu)+2(\rho'+\rho'')\le\lambda/4, \quad \nu-\mu'+\rho''+\lambda-\mu\le\nu.\end{aligned}$$

For example, the choice

$$\lambda=\nu+\left\lfloor\frac{\nu}{20}\right\rfloor \text{ and } \rho'=\rho''=\left\lfloor\frac{\nu}{200}\right\rfloor$$

ensures that the above conditions are satisfied.

Summing up we proved that there exists $\eta'>0$ with

$$S_0 \ll q^{\nu(1-\eta')} \ll N^{1-\eta'}$$

which is precisely the statement of Theorem 1.2.2.

## 4.2 The case $K \not\equiv 0 \bmod 1$

In this section, we show that, for $K = \alpha_0 + \cdots + \alpha_{k-1} \not\equiv 0 \bmod 1$, Proposition 2.2.4 provides an upper bound for the sum

$$S_0 = \sum_{n<N} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell \, \mathrm{s}((n+\ell)^2)\right).$$

Let $\mu$, $\lambda$, $\rho$ and $\rho_1$ be integers satisfying

$$0 \le \rho_1 < \rho < \mu = \nu - 2\rho < \nu < \lambda = \nu + 2\rho < 2\nu \tag{4.13}$$

to be chosen later. Since $K \not\equiv 0 \bmod 1$ we can not use Lemma 3.5.1 directly. Therefore, we apply Lemma 3.2.1 with $Q = 1$ and $R = q^\rho$. Summing trivially for $1 \le r \le R_1 = q^{\rho_1}$ yields

$$|S_0|^2 \ll \frac{N^2 R_1}{R} + \frac{N}{R} \sum_{R_1<r<R} \left(1 - \frac{r}{R}\right) \Re(S_1(r)),$$

where

$$S_1(r) = \sum_{n \in I_1(r)} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell \left(\mathrm{s}((n+\ell)^2) - \mathrm{s}((n+r+\ell)^2)\right)\right)$$

and $I_1(r)$ is an interval included in $[0, N-1]$. By Lemma 3.5.1 we conclude that $\mathrm{s}_{\lambda,\infty}((n+\ell)^2) = \mathrm{s}_{\lambda,\infty}((n+r+\ell)^2)$ for all but $\mathcal{O}(Nq^{-(\lambda-\nu-\rho)})$ values of $n$. Therefore, we see that

$$S_1(r) = S_1'(r) + \mathcal{O}(q^{\nu-(\lambda-\nu-\rho)}),$$

with

$$S_1'(r) = \sum_{n \in I_1(r)} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell \left(\mathrm{s}_\lambda((n+\ell)^2) - \mathrm{s}_\lambda((n+r+\ell)^2)\right)\right).$$

This leads to

$$|S_0|^2 \ll q^{2\nu-\rho+\rho_1} + q^{3\nu+\rho-\lambda} + \frac{q^\nu}{R} \sum_{R_1<r<R} \left|S_1'(r)\right|$$

and, by using the Cauchy-Schwarz inequality to

$$|S_0|^4 \ll q^{4\nu-2\rho+2\rho_1} + q^{6\nu+2\rho-2\lambda} + \frac{q^{2\nu}}{R} \sum_{R_1<r<R} \left|S_1'(r)\right|^2.$$

For $|S_1'(r)|^2$ we can use Lemma 3.2.1 again: Let $\rho' \in \mathbb{N}$ to be chosen later such that $1 \le \rho' \le \rho$. After applying Lemma 3.2.1 with $Q = q^\mu$ and

$$S = q^{2\rho'} \le q^{\nu-\mu}, \tag{4.14}$$

we observe that for any $m \in \mathbb{N}$ we have

$$\mathrm{s}_\lambda((m+sq^\mu)^2) - \mathrm{s}_\lambda(m^2) = \mathrm{s}_{\mu,\lambda}((m+sq^\mu)^2) - \mathrm{s}_{\mu,\lambda}(m^2),$$

and thus

$$|S_0|^4 \ll q^{4\nu-2\rho+2\rho_1} + q^{6\nu+2\rho-2\lambda} + \frac{q^{4\nu}}{S} + \frac{q^{3\nu}}{RS}\sum_{R_1<r<R}\sum_{1\le s<S}|S_2(r,s)|\,, \tag{4.15}$$

with

$$S_2(r,s) = \sum_{n\in I_2(r,s)} \mathrm{e}\Bigg(\sum_{\ell=0}^{k-1}\alpha_\ell\big(\mathrm{s}_{\mu,\lambda}((n+\ell)^2) - \mathrm{s}_{\mu,\lambda}((n+r+\ell)^2) - \mathrm{s}_{\mu,\lambda}((n+sq^\mu+\ell)^2) + \mathrm{s}_{\mu,\lambda}((n+sq^\mu+r+\ell)^2)\big)\Bigg),$$

where $I_2(r,s)$ is an interval included in $[0, N-1]$.

We now make a Fourier analysis similar to the case $K \equiv 0 \bmod 1$.

Let $\mu' = \mu - \rho' > 0$ and

$$U = q^{\lambda-\mu+\rho'},\ U_3 = q^{\nu-\mu+\rho'+1}, V = q^{\lambda-\mu}. \tag{4.16}$$

We again choose the integers $u_1 = u_1(n)$, $u_2 = u_2(n)$, $u_3 = u_3(n)$, $v = v(n)$, $w_1 = w_1(n)$, $w_2 = w_2(n)$, and $w_3 = w_3(n)$ verifying the conditions of Lemma 3.5.2:

$$\begin{aligned}
n^2 &\equiv u_1 q^{\mu'} + w_1 \bmod q^\lambda && (0 \le u_1 < U,\ 0 \le w_1 < q^{\mu'}),\\
(n+r)^2 &\equiv u_2 q^{\mu'} + w_2 \bmod q^\lambda && (0 \le u_2 < U,\ 0 \le w_2 < q^{\mu'}),\\
2n &= u_3 q^{\mu'} + w_3 && (0 \le u_3 < U_3,\ 0 \le w_3 < q^{\mu'}),\\
2sn &\equiv v \bmod q^{\lambda-\mu} && (0 \le v < V),
\end{aligned}$$

Assuming that $\lambda \le 2\mu'$, we have

$$\begin{aligned}
(n+\ell)^2 &\equiv (u_1+\ell u_3)q^{\mu'} + w_1 + \ell w_3 + \ell^2 \bmod q^\lambda,\\
(n+\ell+sq^\mu)^2 &\equiv (u_1+\ell u_3 + vq^{\rho'} + 2\ell s q^{\rho'})q^{\mu'} + w_1 + \ell w_3 + \ell^2 \bmod q^\lambda,\\
(n+\ell+r)^2 &\equiv (u_2+\ell u_3)q^{\mu'} + w_2 + \ell w_3 + \ell^2 + 2r\ell \bmod q^\lambda,\\
(n+\ell+sq^\mu+r)^2 &\equiv (u_2+\ell u_3 + vq^{\rho'} + 2(\ell+r)sq^{\rho'})q^{\mu'} + w_2 + \ell w_3 + \ell^2 + 2r\ell \bmod q^\lambda.
\end{aligned}$$

According to Lemma 3.5.2 for fixed integers $r, s, \ell \ge 1$, the number of integers $n < q^\nu$ for which at least one of the following conditions

$$\begin{aligned}
\mathrm{s}_{\mu,\lambda}((n+\ell)^2) &\ne \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3),\\
\mathrm{s}_{\mu,\lambda}((n+\ell+sq^\mu)^2)) &\ne \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3 + vq^{\rho'} + 2\ell s q^{\rho'})\\
\mathrm{s}_{\mu,\lambda}((n+r+\ell)^2) &\ne \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3),\\
\mathrm{s}_{\mu,\lambda}((n+r+\ell+sq^\mu)^2)) &\ne \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3 + vq^{\rho'} + 2(\ell+r)sq^{\rho'})
\end{aligned}$$

is satisfied is $\ll q^{\nu-\rho'}$. As in Section 4.1 we use characteristic functions to filter the right values

of $u_1$, $u_2$, $u_3$, and obtain

$$\begin{aligned} S_2(r,s) \;=\; & \sum_{0\le u_1<U}\sum_{0\le u_2<U}\sum_{0\le u_3<U_3} \\ & \sum_{n\in I_2(r,s)} \mathrm{e}\Bigg(\sum_{\ell=0}^{k-1}\alpha_\ell\big(\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3)-\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3) \\ & \qquad -\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+v(n)q^{\rho'}+2\ell s q^{\rho'}) \\ & \qquad +\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3+v(n)q^{\rho'}+2(\ell+r)sq^{\rho'})\big)\Bigg) \\ & \chi_{U^{-1}}\left(\frac{n^2}{q^\lambda}-\frac{u_1}{U}\right)\chi_{U^{-1}}\left(\frac{(n+r)^2}{q^\lambda}-\frac{u_2}{U}\right)\chi_{U_3^{-1}}\left(\frac{2n}{q^\nu}-\frac{u_3}{U_3}\right) \\ & +\mathcal{O}(q^{\nu-\rho'}). \end{aligned}$$

Furthermore, we use Lemma 3.1.8 to replace the product of characteristic functions $\chi$ by a product of trigonometric polynomials. Using (3.11) with $U_1 = U_2 = U$, $H_1 = H_2 = Uq^{\rho_2}$ and $H_3 = U_3 q^{\rho_3}$, and integers $\rho_2$, $\rho_3$ verifying

$$\rho_2 \le \mu-\rho',\ \rho_3 \le \mu-\rho', \tag{4.17}$$

we obtain

$$\begin{aligned} S_2(r,s) = S_3(r,s) \;&+\; \mathcal{O}(q^{\nu-\rho'}) + \mathcal{O}\left(E_{30}(r)\right) + \mathcal{O}\left(E_{31}(0)\right) + \mathcal{O}\left(E_{31}(r)\right) \\ &+\; \mathcal{O}\left(E_{32}(0)\right) + \mathcal{O}\left(E_{32}(r)\right) + \mathcal{O}\left(E_{33}(r)\right) + \mathcal{O}\left(E_{34}(r)\right), \end{aligned} \tag{4.18}$$

for the error terms obtained by 3.11

$$\begin{aligned} S_3(r,s) \;=\; & \sum_{0\le u_1<U}\sum_{0\le u_2<U}\sum_{0\le u_3<U_3}\sum_{0\le v<V} \\ & \mathrm{e}\Bigg(\sum_{\ell=0}^{k-1}\alpha_\ell\big(\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3)-\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3) \\ & \qquad -\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+vq^{\rho'}+2\ell s q^{\rho'}) \\ & \qquad +\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3+vq^{\rho'}+2(\ell+r)sq^{\rho'})\big)\Bigg) \\ & \sum_{n\in I_2(r,s)} A_{U^{-1},H_1}\left(\frac{n^2}{q^\lambda}-\frac{u_1}{U}\right)A_{U^{-1},H_2}\left(\frac{(n+r)^2}{q^\lambda}-\frac{u_2}{U}\right)A_{U_3^{-1},H_3}\left(\frac{2n}{q^\nu}-\frac{u_3}{U_3}\right) \\ & \frac{1}{q^{\lambda-\mu}}\sum_{0\le h<q^{\lambda-\mu}}\mathrm{e}\left(h\frac{2sn-v}{q^{\lambda-\mu}}\right). \end{aligned}$$

As in Section 4.1, we use the inner sum to filter the right value for $v$.
Next we estimate the error terms:

$$E_{30}(r) = \frac{U_3}{H_3}q^\nu + \frac{U_3}{H_3}\sum_{1\le h_3'\le H_3/U_3}\left|\sum_{n<q^\nu}\mathrm{e}\left(\frac{2h_3'U_3n}{q^\nu}\right)\right|,$$

which by (3.15) and (4.16) gives

$$E_{30}(r) \ll q^{\nu-\rho_3} + q^{-\rho_3} \sum_{1\le h_3'\le q^{\rho_3}} \left|\sin \frac{2\pi h_3'}{q^{\mu-\rho'-1}}\right|^{-1} \ll q^{\nu-\rho_3} + \mu^{\omega(q)} q^{\mu-\rho'-\rho_3} \ll q^{\nu-\rho_3}$$

where $\omega(q)$ denotes the number of prime divisors of $q$.
Similarly,

$$E_{31}(r) = \frac{U}{H_2} \sum_{|h_2'|\le H_2/U} \left|\sum_{n<q^\nu} \mathrm{e}\left(\frac{h_2'(n+r)^2}{q^\lambda/U}\right)\right|$$

holds. By (3.18) – with $q^{\nu-\mu+\rho'}$ complete sums – (4.9) and (4.17) we conclude

$$\begin{aligned} E_{31}(r) &\ll q^{\nu-\rho_2} + q^{-\rho_2} \sum_{1\le h_2'\le q^{\rho_2}} q^{\nu-\mu+\rho'} \sqrt{\gcd(h_2', q^{\mu-\rho'})} \\ &\ll q^{\nu-\rho_2} + q^{\nu-\mu+\rho'} \ll q^{\nu-\rho_2}. \end{aligned}$$

Next, we consider

$$E_{32}(r) = \frac{U}{H_2}\frac{U_3}{H_3} \sum_{|h_2'|\le H_2/U} \sum_{|h_3'|\le H_3/U_3} \left|\sum_{n<q^\nu} \mathrm{e}\left(\frac{h_2'(n+r)^2}{q^\lambda/U} + \frac{2h_3'n}{q^\nu/U_3}\right)\right|,$$

which can be estimated by (3.18), (4.9) and (4.17), with a trivial summation over $h_3'$:

$$E_{32}(r) \ll q^{\nu-\rho_2} + q^{-\rho_2} \sum_{1\le h_2'\le q^{\rho_2}} q^{\nu-\mu+\rho'} \sqrt{\gcd(h_2', q^{\mu-\rho'})} \ll q^{\nu-\rho_2}.$$

For $E_{33}(r)$ we yield

$$E_{33}(r) = \frac{U^2}{H_2^2} \sum_{|h_1'|\le H_2/U} \sum_{|h_2'|\le H_2/U} \left|\sum_{n<q^\nu} \mathrm{e}\left(\frac{h_1'n^2 + h_2'(n+r)^2}{q^\lambda/U}\right)\right|.$$

Using (3.18), (4.9) and (4.17) as well as substituting $h' = h_1' + h_2'$, we conclude

$$E_{33}(r) \ll q^{\nu-\rho_2} + q^{-\rho_2} \sum_{1\le h'\le q^{\rho_2+1}} q^{\nu-\mu+\rho'} \sqrt{\gcd(h', q^{\mu-\rho'})} \ll q^{\nu-\rho_2}.$$

Similarly, we have

$$E_{34}(r) = \frac{U^2}{H_2^2}\frac{U_3}{H_3} \sum_{|h_1'|\le H_2/U} \sum_{|h_2'|\le H_2/U} \sum_{|h_3'|\le H_3/U_3} \left|\sum_{n<q^\nu} \mathrm{e}\left(\frac{h_1'n^2 + h_2'(n+r)^2}{q^\lambda/U} + \frac{2h_3'n}{q^\nu/U_3}\right)\right|,$$

and, by (3.18), (4.9) and (4.17), substituting $h' = h_1' + h_2'$, with a trivial summation over $h_3'$, we get

$$E_{34}(r) \ll q^{\nu-\rho_2} + q^{-\rho_2} \sum_{1\le h'\le q^{\rho_2+1}} q^{\nu-\mu+\rho'} \sqrt{\gcd(h', q^{\mu-\rho'})} \ll q^{\nu-\rho_2}.$$

In conclusion we deduce that

$$S_2(r,s) = S_3(r,s) + \mathcal{O}(q^{\nu-\rho'}) + \mathcal{O}(q^{\nu-\rho_2}) + \mathcal{O}(q^{\nu-\rho_3}). \tag{4.19}$$

We now reformulate $S_3(r,s)$ by expanding the trigonometric polynomials. Restructuring yields

$$\begin{aligned} S_3(r,s) \;=\; & \frac{1}{q^{\lambda-\mu}} \sum_{0\le h<q^{\lambda-\mu}} \sum_{|h_1|\le H_1} a_{h_1}(U^{-1},H_1) \sum_{|h_2|\le H_2} a_{h_2}(U^{-1},H_2) \sum_{|h_3|\le H_3} a_{h_3}(U_3^{-1},H_3) \\ & \sum_{0\le u_1<U} \sum_{0\le u_2<U} \sum_{0\le u_3<U_3} \sum_{0\le v<V} \mathrm{e}\left(-\frac{h_1u_1+h_2u_2}{U} - \frac{h_3u_3}{U_3} - \frac{hv}{q^{\lambda-\mu}}\right) \\ & \mathrm{e}\Bigg(\sum_{\ell=0}^{k-1} \alpha_\ell \big(\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3) - \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3) \\ & \qquad - \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+vq^{\rho'}+2\ell s q^{\rho'}) \\ & \qquad + \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3+vq^{\rho'}+2(\ell+r)sq^{\rho'})\big)\Bigg) \\ & \sum_{n\in I_2(r,s)} \mathrm{e}\left(\frac{h_1n^2+h_2(n+r)^2}{q^\lambda} + \frac{2h_3n}{q^\nu} + \frac{2hsn}{q^{\lambda-\mu}}\right). \end{aligned}$$

We now split the sum $S_3(r,s)$ into two parts:

$$S_3(r,s) = S_4(r,s) + S_4'(r,s), \tag{4.20}$$

where $S_4(r,s)$ denotes the contribution of the terms for which $h_1+h_2=0$ while $S_4'(r,s)$ denotes the contribution of the terms for which $h_1+h_2\neq 0$. We have by (3.19)

$$\begin{aligned} S_4'(r,s) \;&\ll\; \sum_{|h_1|\le H_1} a_{h_1}(U^{-1},H_1) \sum_{|h_2|\le H_2} a_{h_2}(U^{-1},H_2) \sum_{|h_3|\le H_3} a_{h_3}(U_3^{-1},H_3) \\ &\qquad U^2U_3V\lambda q^{\lambda/2}\sqrt{\gcd(h_1+h_2,q^\lambda)} \\ &\ll\; \nu^3U^2U_3V\lambda q^{\lambda/2}\sqrt{2H_2} \\ &\ll\; \nu^4 q^{\nu+\frac{1}{2}(8\lambda-9\mu+7\rho'+\rho_2)}. \end{aligned}$$

Therefore it remains to consider $S_4(r,s)$. Setting $u_1 = u_1'' + q^{\rho'}u_1'$, $u_2 = u_2'' + q^{\rho'}u_2'$ and $u_3 = u_3'' + q^{\rho'}u_3'$, (where $0 \le u_1'', u_2'', u_3'' < q^{\rho'}$) we can replace the two-fold restricted sum of digits functions by a truncated sum of digits functions

$$\begin{aligned} \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3) &= \mathrm{s}_{\lambda-\mu}\left(u_1'+\ell u_3'+\left\lfloor (u_1''+\ell u_3'')/q^{\rho'}\right\rfloor\right), \\ \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3) &= \mathrm{s}_{\lambda-\mu}\left(u_2'+\ell u_3'+\left\lfloor (u_2''+\ell u_3'')/q^{\rho'}\right\rfloor\right), \\ \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+vq^{\rho'}+2\ell sq^{\rho'}) &= \mathrm{s}_{\lambda-\mu}\left(u_1'+v+\ell(u_3'+2s)+\left\lfloor (u_1''+\ell u_3'')/q^{\rho'}\right\rfloor\right) \\ \mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3+vq^{\rho'}+2(\ell+r)sq^{\rho'}) &= \mathrm{s}_{\lambda-\mu}\left(u_2'+v+2sr+\ell(u_3'+2s)+\left\lfloor (u_2''+\ell u_3'')/q^{\rho'}\right\rfloor\right). \end{aligned}$$

Using the periodicity modulo $V := q^{\lambda-\mu}$, we replace the variable $v$ by $v_1$ such that $v_1 \equiv u_1' + v \bmod q^{\lambda-\mu}$. Furthermore we introduce a new variable $v_2$ such that

$$v_2 \equiv u_2' + v + 2sr \equiv v_1 + u_2' - u_1' + 2sr \bmod q^{\lambda-\mu}.$$

If we observe that $U/q^{\rho'} = V$ and write $U_3' = U_3/q^{\rho'}$, we obtain a slightly messy formula for $S_4(r,s)$ which yields a good estimation for $S_4(r,s)$. We use a summation over $h$ to filter the right value of $v_1$ and a summation over $h'$ to filter the right value of $v_2$.

$$\begin{aligned}
S_4(r,s) \;=\; & q^{2\mu-2\lambda} \sum_{0\le h<q^{\lambda-\mu}} \sum_{0\le h'<q^{\lambda-\mu}} \sum_{|h_2|\le H_2} a_{-h_2}(U^{-1},H_2)a_{h_2}(U^{-1},H_2) \sum_{|h_3|\le H_3} a_{h_3}(U_3^{-1},H_3) \\
& \sum_{0\le u_1''<q^{\rho'}} \sum_{0\le u_2''<q^{\rho'}} \sum_{0\le u_3''<q^{\rho'}} \mathrm{e}\left(-\frac{-h_2u_1''+h_2u_2''}{U} - \frac{h_3u_3''}{U_3}\right) \\
& \sum_{0\le u_3'<U_3'} \mathrm{e}\left(-\frac{h_3u_3'}{U_3'} + \frac{2h'sr}{q^{\lambda-\mu}}\right) \\
& \sum_{0\le u_1'<V} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell \,\mathrm{s}_{\lambda-\mu}\left(u_1' + \ell u_3' + \left\lfloor (u_1''+\ell u_3'')/q^{\rho'}\right\rfloor\right) - \frac{(-h_2-h+h')u_1'}{q^{\lambda-\mu}}\right) \\
& \sum_{0\le u_2'<V} \mathrm{e}\left(-\sum_{\ell=0}^{k-1} \alpha_\ell \,\mathrm{s}_{\lambda-\mu}\left(u_2' + \ell u_3' + \left\lfloor (u_2''+\ell u_3'')/q^{\rho'}\right\rfloor\right) + \frac{(h'-h_2)u_2'}{q^{\lambda-\mu}}\right) \\
& \sum_{0\le v_1<V} \mathrm{e}\left(-\sum_{\ell=0}^{k-1} \alpha_\ell \,\mathrm{s}_{\lambda-\mu}\left(v_1 + \ell(u_3'+2s) + \left\lfloor (u_1''+\ell u_3'')/q^{\rho'}\right\rfloor\right) + \frac{(h'-h)v_1}{q^{\lambda-\mu}}\right) \\
& \sum_{0\le v_2<V} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell \,\mathrm{s}_{\lambda-\mu}\left(v_2 + \ell(u_3'+2s) + \left\lfloor (u_2''+\ell u_3'')/q^{\rho'}\right\rfloor\right) - \frac{h'v_2}{q^{\lambda-\mu}}\right) \\
& \sum_{n\in I_2(r,s)} \mathrm{e}\left(\frac{2h_2rn+h_2r^2}{q^\lambda} + \frac{2h_3n}{q^\nu} + \frac{2hsn}{q^{\lambda-\mu}}\right).
\end{aligned}$$

Using (2.4), we yield

$$\begin{aligned}
S_4(r,s) \;\ll\; & q^{2\lambda-2\mu} \sum_{0\le h<q^{\lambda-\mu}} \sum_{0\le h'<q^{\lambda-\mu}} \sum_{|h_2|\le H_2} \min(U^{-2},h_2^{-2}) \sum_{|h_3|\le H_3} \min(U_3^{-1},h_3^{-1}) \\
& \sum_{0\le u_1''<q^{\rho'}} \sum_{0\le u_2''<q^{\rho'}} \sum_{0\le u_3''<q^{\rho'}} \sum_{0\le u_3'<U_3'} \\
& \left|G_{\lambda-\mu}^{I(u_1'',u_3'')}(h'-h-h_2,u_3')\right| \left|G_{\lambda-\mu}^{I(u_2'',u_3'')}(h'-h_2,u_3')\right| \\
& \left|G_{\lambda-\mu}^{I(u_1'',u_3'')}(h'-h,u_3'+2s)\right| \left|G_{\lambda-\mu}^{I(u_2'',u_3'')}(h',u_3'+2s)\right| \\
& \left|\sum_{n\in I_2(r,s)} \mathrm{e}\left(\frac{2h_2rn}{q^\lambda} + \frac{2h_3n}{q^\nu} + \frac{2hsn}{q^{\lambda-\mu}}\right)\right|,
\end{aligned}$$

with

$$I(u,\tilde{u}) = \left( \left\lfloor \frac{u}{q^{\rho'}} \right\rfloor, \left\lfloor \frac{u+\tilde{u}}{q^{\rho'}} \right\rfloor, \ldots, \left\lfloor \frac{u+(k-1)\tilde{u}}{q^{\rho'}} \right\rfloor \right) \quad \text{for } (u,\tilde{u}) \in \mathbb{N}^2.$$

Bounding the sum over $n$ by (3.13), leads to

$$\begin{aligned} S_4(r,s) \;\ll\; & q^{2\lambda-2\mu} \sum_{0\le u_1'',u_2'',u_3''<q^{\rho'}} \sum_{|h_2|\le H_2} \min(U^{-2},h_2^{-2}) \sum_{|h_3|\le H_3} \min(U_3^{-1},h_3^{-1}) \\ & \sum_{0\le h<q^{\lambda-\mu}} \left| \min\left( q^{\nu}, \left| \sin \pi \frac{2h_2 r + 2q^{\lambda-\nu}h_3 + 2q^{\mu}hs}{q^{\lambda}} \right|^{-1} \right) \right| S_5(h,h_2,s,u_1'',u_2'',u_3''), \end{aligned}$$

where

$$\begin{aligned} S_5(h,h_2,s,u_1'',u_2'',u_3'') \;:=\; & \sum_{0\le u_3'<U_3'} \sum_{0\le h'<q^{\lambda-\mu}} \left| G_{\lambda-\mu}^{I(u_1'',u_3'')}(h'-h-h_2,u_3') \right| \left| G_{\lambda-\mu}^{I(u_2'',u_3'')}(h'-h_2,u_3') \right| \\ & \left| G_{\lambda-\mu}^{I(u_1'',u_3'')}(h'-h,u_3'+2s) \right| \left| G_{\lambda-\mu}^{I(u_2'',u_3'')}(h',u_3'+2s) \right|. \end{aligned}$$

This sum can be bounded from above by using the Cauchy-Schwarz inequality:

$$\begin{aligned} & S_5(h,h_2,s,u_1'',u_2'',u_3'') \\ & \le \left( \sum_{0\le u_3'<U_3'} \sum_{0\le h'<q^{\lambda-\mu}} \left| G_{\lambda-\mu}^{I(u_1'',u_3'')}(h'-h-h_2,u_3') \right|^2 \left| G_{\lambda-\mu}^{I(u_1'',u_3'')}(h'-h,u_3'+2s) \right|^2 \right)^{1/2} \\ & \quad \left( \sum_{0\le u_3'<U_3'} \sum_{0\le h'<q^{\lambda-\mu}} \left| G_{\lambda-\mu}^{I(u_2'',u_3'')}(h'-h_2,u_3') \right|^2 \left| G_{\lambda-\mu}^{I(u_2'',u_3'')}(h',u_3'+2s) \right|^2 \right)^{1/2}. \end{aligned}$$

By periodicity modulo $q^{\lambda-\mu}$ and taking $h''=h'-h$, the first parenthesis is independent of $h$ and we get

$$S_5(h,h_2,s,u_1'',u_2'',u_3'') \le S_6(h_2,s,u_1'',u_3'')^{1/2} S_6(h_2,s,u_2'',u_3'')^{1/2},$$

with

$$S_6(h_2,s,u'',u_3'') = \sum_{0\le u_3'<U_3'} \sum_{0\le h'<q^{\lambda-\mu}} \left| G_{\lambda-\mu}^{I(u'',u_3'')}(h'-h_2,u_3') \right|^2 \left| G_{\lambda-\mu}^{I(u'',u_3'')}(h',u_3'+2s) \right|^2. \quad (4.21)$$

We obtain

$$\begin{aligned} S_4(r,s) \;\ll\; & q^{2\lambda-2\mu} \sum_{0\le u_1'',u_2'',u_3''<q^{\rho'}} \sum_{|h_2|\le H_2} \min(U^{-2},h_2^{-2}) \sum_{|h_3|\le H_3} \min(U_3^{-1},h_3^{-1}) \\ & S_6(h_2,s,u_1'',u_3'')^{1/2} S_6(h_2,s,u_2'',u_3'')^{1/2} \\ & \sum_{0\le h<q^{\lambda-\mu}} \left| \min\left( q^{\nu}, \left| \sin \pi \frac{2h_2 r + q^{\lambda-\nu}2h_3 + q^{\mu}2hs}{q^{\lambda}} \right|^{-1} \right) \right|. \end{aligned}$$

Assuming

$$\lambda - 2\mu + \rho' + \rho_2 + \rho \le -3, \lambda - 2\mu + \rho' + \rho_3 + 1 \le -3 \tag{4.22}$$

we can verify

$$\left|2h_2 r + q^{\lambda-\nu} 2h_3\right| / q^\mu \le (2H_2 R + q^{\lambda-\nu} 2H_3)/q^\mu \le 2q^{\lambda-2\mu+\rho'+\rho_2+\rho} + 2q^{\lambda-2\mu+\rho'+\rho_3+1} \le 1/2,$$

and thus we can actually use the sharper bound in (3.14) to bound the inner sum:

$$\begin{aligned}
&\sum_{0\le h<q^{\lambda-\mu}} \left|\min\left(q^\nu, \left|\sin \pi \frac{2h_2 r + 2q^{\lambda-\nu} h_3 + q^\mu 2hs}{q^\lambda}\right|^{-1}\right)\right| \\
&\quad \ll \quad \gcd(2s, q^{\lambda-\mu}) \min\left(q^\nu, \left|\sin \pi \tfrac{2h_2 r + 2q^{\lambda-\nu} h_3}{q^\lambda}\right|^{-1}\right) + (\lambda-\mu) q^{\lambda-\mu}.
\end{aligned}$$

Since $q^{\lambda-\mu} \ll \min\left(q^\nu, \left|\sin \pi \frac{2h_2 r + 2q^{\lambda-\nu} h_3}{q^\lambda}\right|^{-1}\right)$, it follows

$$\begin{aligned}
S_4(r,s) \quad \ll \quad (\lambda-\mu)\ \gcd(2s, q^{\lambda-\mu})\ q^{2\lambda-2\mu} &\sum_{0\le u_1'', u_2'', u_3'' < q^{\rho'}} \sum_{|h_2|\le H_2} \min(U^{-2}, h_2^{-2}) \\
&S_6(h_2, s, u_1'', u_3'')^{1/2} S_6(h_2, s, u_2'', u_3'')^{1/2} \\
&\sum_{|h_3|\le H_3} \min(U_3^{-1}, h_3^{-1}) \min\left(q^\nu, \left|\sin \pi \tfrac{2h_2 r + 2q^{\lambda-\nu} h_3}{q^\lambda}\right|^{-1}\right).
\end{aligned}$$

Here we recall that in (4.15) we have $R_1 < r < R$ and thus introduce the integers $H_2'$ and $\kappa$ such that

$$H_2' = q^{\lambda-\nu+1} H_3 / R_1 = q^{\lambda-\mu+\rho'+\rho_3-\rho_1+2} = q^\kappa. \tag{4.23}$$

Assuming that

$$\rho' + \rho_3 + 2 < \rho_1, \tag{4.24}$$

we have $H_2' < q^{\lambda-\mu}$ by (4.16) and the condition $|h_2| > H_2'$ ensures that $q^{\lambda-\nu}|h_3| \le \frac{1}{2}|h_2 r|$. This leads to

$$S_4(r,s) \ll S_{41}(r,s) + S_{42}(r,s) + S_{43}(r,s),$$

where $S_{41}(r,s)$, $S_{42}(r,s)$ and $S_{43}(r,s)$ denote the contribution of the terms $|h_2| \le H_2'$, $H_2' < |h_2| \le q^{\lambda-\mu}$ and $q^{\lambda-\mu} < |h_2| \le H_2$ respectively.

This separation allows us to deal with very low values of $|h_2|$ in $S_{41}$, and thus we can use (3.14) efficiently. We have already seen that, $q^{\lambda-\mu}|h_3| \le \frac{1}{2}|h_2 r|$ holds for $|h_2| > H_2'$ and, therefore,

$$\min\left(q^\nu, \left|\sin \pi \tfrac{2h_2 r + 2q^{\lambda-\nu} h_3}{q^\lambda}\right|^{-1}\right) \ll \frac{q^\lambda}{H_2' r}.$$

For $S_{43}$ we split the sum into parts of length $q^{\lambda-\mu}$ to be able to find an appropriate estimate.

**Estimate of $S_{41}(r,s)$** By (3.14) we have

$$\sum_{|h_3|\le H_3} \min\left(q^\nu, \left|\sin \pi \tfrac{2h_3+2h_2 r q^{\nu-\lambda}}{q^\nu}\right|^{-1}\right) \ll \nu q^\nu,$$

and, therefore,

$$S_{41}(r,s) \ll \nu\,(\lambda-\mu)\ \gcd(2s, q^{\lambda-\mu})\ q^{\nu+2\lambda-2\mu} U^{-2} U_3^{-1} \sum_{0\le u_1'', u_2'', u_3'' < q^{\rho'}} \sum_{|h_2|\le H_2'} S_6(h_2, s, u_1'', u_3'')^{1/2} S_6(h_2, s, u_2'', u_3'')^{1/2}.$$

By Proposition 2.2.4 (replacing $\lambda$ by $\lambda-\mu$ and $L$ by $\lambda-\mu-\kappa$), we find some $0<\eta'\le 1$ such that

$$\left|G_{\lambda-\mu}^{I(u'',u_3'')}(h'-h_2, u_3')\right| \ll q^{-\eta'(\lambda-\mu-\kappa)} \max_{J\in\mathcal{I}_k} \left|G_\kappa^J(h'-h_2, \lfloor u_3'/q^L\rfloor)\right|.$$

By Parseval's equality and recalling that $\#(\mathcal{I}_k) = 2^{k-1}$, it follows that

$$\sum_{|h_2|\le H_2'} \max_{J\in\mathcal{I}_k} \left|G_\kappa^J \lfloor (h'-h_2, u_3'/q^L\rfloor)\right|^2 \le \sum_{J\in\mathcal{I}_k} \sum_{|h_2|\le H_2'} \left|G_\kappa^J(h'-h_2, \lfloor u_3'/q^L\rfloor)\right|^2 \le 2^{k-1}.$$

We obtain

$$\sum_{|h_2|\le H_2'} \left|G_{\lambda-\mu}^{I(u'',u_3'')}(h'-h_2, u_3')\right|^2 \ll q^{-\eta'(\lambda-\mu-\kappa)} = \left(\frac{H_2'}{q^{\lambda-\mu}}\right)^{\eta'}$$

uniformly in $\lambda$, $\mu$, $H_2'$, $u_3'$, $u''$ and $u_3''$. It follows from (4.21) and Parseval's equality that

$$\sum_{|h_2|\le H_2'} S_6(h_2, s, u'', u_3'') \ll U_3' \left(\frac{H_2'}{q^{\lambda-\mu}}\right)^{2\eta'}.$$

By the Cauchy-Schwarz inequality, we obtain

$$\sum_{|h_2|\le H_2'} S_6(h_2, s, u_1'', u_3'')^{1/2} S_6(h_2, s, u_2'', u_3'')^{1/2} \le \left(\sum_{|h_2|\le H_2'} S_6(h_2, s, u_1'', u_3'')\right)^{1/2} \left(\sum_{|h_2|\le H_2'} S_6(h_2, s, u_2'', u_3'')\right)^{1/2} \ll U_3' \left(\frac{H_2'}{q^{\lambda-\mu}}\right)^{2\eta'}.$$

This, finally, yields

$$S_{41}(r,s) \ll \nu\,(\lambda-\mu)\ \gcd(2s, q^{\lambda-\mu})\ q^{\nu+2\lambda-2\mu+3\rho'} U^{-2} U_3^{-1} U_3' \left(\frac{H_2'}{q^{\lambda-\mu}}\right)^{2\eta'},$$

and, by (4.23), (4.16) and (3.17), we find

$$\frac{1}{RS} \sum_{R_1<r<R} \sum_{1\le s<S} S_{41}(r,s) \ll \nu\,(\lambda-\mu)^{\omega(q)+1}\ q^{\nu-2\eta'(\rho_1-\rho'-\rho_3)}, \tag{4.25}$$

which concludes this part.

**Estimate of $S_{42}(r,s)$** The condition $|h_2| > H_2'$ ensures that $q^{\lambda-\nu}|h_3| \le \frac{1}{2}|h_2 r|$ and

$$\min\left(q^\nu, \left|\sin \pi \tfrac{2h_2 r + 2q^{\lambda-\nu}h_3}{q^\lambda}\right|^{-1}\right) \ll \frac{q^\lambda}{H_2' r}.$$

We obtain, similar as in the estimation of $S_{41}(r,s)$, by Parseval's equality

$$\sum_{|h_2|\le H_2'} \left|G_{\lambda-\mu}^{I(u'',u_3'')}(h'-h_2,u_3')\right|^2 \le \sum_{J\in\mathcal{I}_k} \left|G_{\lambda-\mu}^{J}(h'-h_2,u_3')\right|^2 \ll 1$$

and therefore – again by Parseval's equality –

$$\sum_{|h_2|\le H_2'} S_6(h_2,s,u'',u_3'') \ll U_3'.$$

By the Cauchy-Schwarz inequality, we have

$$\begin{aligned}&\sum_{H_2'<|h_2|\le q^{\lambda-\mu}} S_6(h_2,s,u_1'',u_3'')^{1/2} S_6(h_2,s,u_2'',u_3'')^{1/2}\\ &\le \left(\sum_{|h_2|\le q^{\lambda-\mu}} S_6(h_2,s,u_1'',u_3'')\right)^{1/2}\left(\sum_{|h_2|\le q^{\lambda-\mu}} S_6(h_2,s,u_2'',u_3'')\right)^{1/2} \ll U_3'.\end{aligned}$$

It follows that

$$S_{42}(r,s) \ll (\lambda-\mu)\ \gcd(2s,q^{\lambda-\mu})\ q^{2\lambda-2\mu+3\rho'}U^{-2}\frac{q^\lambda}{H_2' r}U_3' \sum_{|h_3|\le H_3} \min(U_3^{-1},h_3^{-1})$$

and we get, by (4.23) and (4.16),

$$S_{42}(r,s) \ll (\lambda-\mu)\ \frac{\gcd(2s,q^{\lambda-\mu})}{r} q^{\nu+\rho-\rho_3}\rho_3.$$

By (3.17), we yield

$$\frac{1}{RS}\sum_{R_1<r<R}\sum_{1\le s<S} S_{42}(r,s) \ll \rho\rho_3(\lambda-\mu)^{1+\omega(q)}\ q^{\nu-\rho_3}. \tag{4.26}$$

**Estimate of $S_{43}(r,s)$** We split the summation over $h_2$ into $J := H_2/q^{\lambda-\mu} - 1$ parts of the form

$$jq^{\lambda-\mu} < h_2 \le (j+1)q^{\lambda-\mu} \text{ with } j = 1,\dots,J.$$

The condition $|h_2| > jq^{\lambda-\mu}$ ensures that $q^{\lambda-\nu}|h_3| \le \frac{1}{2}|h_2 r|$ and thus

$$\min\left(q^\nu, \left|\sin \pi \tfrac{2h_2 r + 2q^{\lambda-\nu}h_3}{q^\lambda}\right|^{-1}\right) \ll \frac{q^\lambda}{jq^{\lambda-\mu}r} = \frac{q^\mu}{jr}.$$

By the Cauchy-Schwarz inequality, we have – by the same argument as above –

$$\sum_{jq^{\lambda-\mu}<|h_2|\leq(j+1)q^{\lambda-\mu}} S_6(h_2,s,u_1'',u_3'')^{1/2} S_6(h_2,s,u_2'',u_3'')^{1/2}$$
$$\ll \left(\sum_{h_2 \bmod q^{\lambda-\mu}} S_6(h_2,s,u_1'',u_3'')\right)^{1/2} \left(\sum_{h_2 \bmod q^{\lambda-\mu}} S_6(h_2,s,u_2'',u_3'')\right)^{1/2} \ll U_3'.$$

It follows that

$$S_{43}(r,s) \ll (\lambda-\mu)\ \gcd(2s,q^{\lambda-\mu})\ q^{3\rho'} U_3' \sum_{1\leq j\leq J} \frac{q^\mu}{j^3 r} \sum_{|h_3|\leq H_3} \min(U_3^{-1}, h_3^{-1}),$$

and by (4.16) and (3.17) we finally yield

$$\frac{1}{RS} \sum_{R_1<r<R} \sum_{1\leq s<S} S_{43}(r,s) \ll \rho\ (\lambda-\mu)^{1+\omega(q)}\ q^{\nu-\rho+3\rho'}. \tag{4.27}$$

**Combining the estimates for $S_4$** It follows from (4.25), (4.26) and (4.27) that

$$\frac{1}{RS} \sum_{R_1<r<R} \sum_{1\leq s<S} S_4(r,s) \ll \nu^{3+\omega(q)} q^\nu \left(q^{-2\eta'(\rho_1-\rho'-\rho_3)} + q^{-\rho_3} + q^{-\rho+3\rho'}\right).$$

Choosing

$$\rho_1 = \rho-\rho',\ \rho_2=\rho_3=\rho',$$

we obtain

$$\frac{1}{RS} \sum_{R_1<r<R} \sum_{1\leq s<S} S_4(r,s) \ll \nu^{3+\omega(q)} q^\nu \left(q^{-2\eta'(\rho-3\rho')} + q^{-\rho'} + q^{-(\rho-3\rho')}\right).$$

Since $0<\eta'<1$, we obtain using (4.20) and (4.19), that

$$\frac{1}{RS} \sum_{R_1<r<R} \sum_{1\leq s<S} S_2(r,s) \ll \nu^{3+\omega(q)} q^\nu \left(q^{-\eta'(\rho-3\rho')} + q^{-\rho'} + q^{\frac{1}{2}(8\lambda-9\mu+8\rho')}\right).$$

We recall by (4.14) that $S=q^{2\rho'}$ and by (4.13) that $\mu=\nu-2\rho$, $\lambda=\nu+2\rho$ and insert the estimation from above in (4.15):

$$|S_0|^4 \ll q^{4\nu-2\rho'} + q^{4\nu-2\rho} + \nu^{3+\omega(q)} q^{4\nu} \left(q^{-\eta'(\rho-3\rho')} + q^{-\rho'} + q^{-\frac{\nu}{2}+17\rho+4\rho'}.\right)$$

For $\rho' = \lfloor \nu/146 \rfloor$ and $\rho = 4\rho'$, we obtain

$$|S_0| \ll \nu^{(3+\omega(q))/4} q^{\nu-\frac{\eta'\rho'}{4}} \ll \nu^{(3+\omega(q))/4} N^{1-\eta''}.$$

Therefore we have seen that Proposition 2.2.4 implies the case $K \not\equiv 0 \bmod 1$ of Theorem 1.2.2.

# Conclusion

At last, we comment on possible generalizations of the covered problem.

A natural generalization would be to consider quadratic polynomials instead of $n^2$. The author suspects that the developed methods can also be applied in this case without major changes. For higher-degree polynomials, it would be necessary to generalize the results on carry propagation in Chapter 3 and find estimates for cubic and higher-degree exponential sums which are not covered by this thesis. However, it is not yet known whether the asymptotic distribution along cubic polynomials is uniform.

Another possible generalization is to consider $q$-additive functions instead of $s_q$ (still along $n^2$). Chapter 3 can be adapted to $q$-additive functions by only minor changes. However, the results from Sections 2.3 and 2.4 can not be generalized in a trivial way. Provided these generalizations, the proof of the main theorem follows easily.

A generalization of $q$-additive functions are (invertible) automatic sequences. It is known by [18] that the asymptotic frequencies along squares exist, but no quantitative statement has yet been found.

One sees that there are still many open problems as well as uncovered aspects of Gelfond's third problem. Some sub-problems might possibly be solved soon, but there still remains enough room for improvements and further research.

# Bibliography


[1] J.-P. Allouche and J. Shallit.
*Automatic sequences.*
Cambridge University Press, Cambridge, 2003.
Theory, applications, generalizations.

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

[3] M. Drmota, C. Mauduit, and J. Rivat.
The thue-morse sequence along squares is normal.
manuscript.

[4] M. Drmota, C. Mauduit, and J. Rivat.
The sum-of-digits function of polynomial sequences.
*J. Lond. Math. Soc. (2)*, 84(1):81–102, 2011.

[5] M. Drmota and J. F. Morgenbesser.
Generalized Thue-Morse sequences of squares.
*Israel J. Math.*, 190:157–193, 2012.

[6] A. O. Gelfond.
Sur les nombres qui ont des propriétés additives et multiplicatives données.
*Acta Arith.*, 13:259–265, 1967/1968.

[7] S. W. Graham and G. Kolesnik.
*Van der Corput's method of exponential sums*, volume 126 of *London Mathematical Society Lecture Note Series.*
Cambridge University Press, Cambridge, 1991.

[8] P. Hrsg. v. Kritzer, H. Niederreiter, F. Pillichshammer, and A. Winterhof.
Proceedings ricam workshop "uniform distribution and quasi-monte carlo methods".
*DeGruyter*, 15:87–104, 2014.

[9] D.-H. Kim.
On the joint distribution of $q$-additive functions in residue classes.
*J. Number Theory*, 74(2):307–336, 1999.

[10] C. Mauduit.
Multiplicative properties of the Thue-Morse sequence.
*Period. Math. Hungar.*, 43(1-2):137–153, 2001.

[11] C. Mauduit and J. Rivat.
La somme des chiffres des carrés.
*Acta Math.*, 203(1):107–148, 2009.

[12] C. Mauduit and J. Rivat.
La somme des chiffres des carrés.
*Acta Math.*, 203(1):107–148, 2009.

[13] C. Mauduit and J. Rivat.
Sur un problème de Gelfond: la somme des chiffres des nombres premiers.

*Ann. of Math. (2)*, 171(3):1591–1646, 2010.

[14] J. Morgenbesser.
Gelfond's sum of digits problems, 2008.
Wien, Techn. Univ., Dipl.-Arb., 2008.

[15] H. M. Morse.
Recurrent geodesics on a surface of negative curvature.
*Trans. Amer. Math. Soc.*, 22(1):84–100, 1921.

[16] A. Thue.
Über unendliche zeichenreihen.
*Norske vid. Selsk. Skr. Mat. Nat. Kl.*, 7:1–22, 1906.

[17] A. Thue.
*Ueber die gegenseitige Lage gleicher Teile gewisser Zeichenreihen.*
Skrifter. Jac. Dybwad, 1912.

[18] J. D. Vaaler.
Some extremal functions in Fourier analysis.
*Bull. Amer. Math. Soc. (N.S.)*, 12(2):183–216, 1985.