Canad. J. Math. Vol. 70 (5), 2018 pp. 1096–1129
http://dx.doi.org/10.4153/CJM-2017-053-1

The Rudin–Shapiro Sequence and Similar Sequences Are Normal Along Squares

Clemens Müllner

Abstract. We prove that digital sequences modulo m along squares are normal, which covers some prominent sequences, such as the sum of digits in base q modulo m, the Rudin–Shapiro sequence, and some generalizations. This gives, for any base, a class of explicit normal numbers that can be efficiently generated.

1 Introduction

This paper deals with digital sequences modulo m. Such sequences are "simple" in the sense that they are deterministic and uniformly recurrent sequences. We show that the situation changes completely when we consider the subsequence along squares, *i.e.*, we show that this subsequence is normal. Thus, we describe a new class of normal numbers that can be efficiently generated, *i.e.*, the first n digits of the normal number can be generated by using $O(n\log(n))$ elementary operations.

In this paper we let $\mathbb{N}$ denote the set of positive integers and we let $\mathbb{P}$ denote the set of prime numbers. We let $\mathbb{U}$ denote the set of complex numbers of modulus 1 and we use the abbreviation $\mathrm{e}(x) = \exp(2\pi i x)$ for any real number x. For two functions, f and g that take only strictly positive real values, we write $f = O(g)$ or $f \ll g$ if f/g is bounded. We let $\lfloor x \rfloor$ denote the floor function and $\{x\}$ denote the fractional part of x. Furthermore, we let $\chi_\alpha(x)$ denote the indicator function for $\{x\}$ in $[0,\alpha)$. Moreover, we let $\tau(n)$ denote the number of divisors of n, $\omega(n)$ denote the number of distinct prime factors of n, and $\varphi(n)$ denote the number of positive integers smaller than n that are co-prime to n. Furthermore, let $\varepsilon_j^{(q)}(n) \in \{0,\dots,q-1\}$ denote the j-th digit in the base q expansion of a non-negative integer n, *i.e.*, $n = \sum_{j=0}^{r} \varepsilon_j^{(q)}(n) q^j$, where $r = \lfloor \log_q(n) \rfloor$. We usually omit the superscript, as we work with arbitrary but fixed base $q \geq 2$.

1.1 Digital Sequences

The main topic of this paper is digital sequences modulo m'. We use a slightly different definition of digital function than the one found in [1].

Received by the editors May 9, 2017; revised November 3, 2017.
Published electronically April 30, 2018.
This research was supported by the project F55-02 of the Austrian Science Fund FWF, part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications", by Project F5002-N15 (FWF), part of the Special Research Program Algorithmic and Enumerative Combinatorics, and by Project I1751 (FWF), called MUDERA (Multiplicativity, Determinism, and Randomness).
AMS subject classification: **11A63**, 11B85, 11L03, 11N60, 60F05.
Keywords: Rudin–Shapiro sequence, digital sequences, normality, exponential sums.

Definition 1.1 We call a function $b\colon \mathbb{N} \to \mathbb{N}$ a *strongly block-additive q-ary function* or *digital function* if there exist $m \in \mathbb{N}_{>0}$ and $F\colon \{0,\dots,q-1\}^m \to \mathbb{N}$ such that $F(0,\dots,0) = 0$ and $b(n) = \sum_{j\in\mathbb{Z}} F(\varepsilon_{j+m-1}^{(q)}(n),\dots,\varepsilon_j^{(q)}(n))$, where we define $\varepsilon_{-j}(n) = 0$ for all $j \geq 1$.

The difference from the usual definition is the range of the sum ($\mathbb{N}_0$ or $\mathbb{Z}$) which does not matter for all appearing examples.

Remark 1.2 The name strongly block-additive q-ary function was inspired by (strongly) q-additive functions. Bellman and Shapiro [3] and Gelfond [9] denoted a function f to be q-additive if $f(aq^r+b) = f(aq^r)+f(b)$ holds for all $r \geq 1$, $1 \leq a < q$, and $0 \leq b < q^r$. Mendès France [14] denoted a function f to be strongly q-additive if $f(aq^r+b) = f(a)+f(b)$ holds for all $r \geq 1$, $1 \leq a < q$, and $0 \leq b < q^r$. Thus, for a strongly q-additive function f, we can write $f(n) = \sum_{j\in\mathbb{Z}} f(\varepsilon_j^{(q)}(n))$.

A quite prominent example of a strongly block-additive function is the sum of digits function $s_q(n)$ in base q. This is a strongly block-additive function with $m = 1$ and $F(x) = x$. In particular, $(s_2(n) \bmod 2)_{n\in\mathbb{N}}$ gives the well-known Thue–Morse sequence.

Another prominent example is the Rudin–Shapiro sequence $\mathbf{r} = (r_n)_{n\geq 0}$ which is given by the parity of the number of blocks of the form "11" in the digital expansion in base 2. Let b be the digital sequence corresponding to $q = 2$, $m = 2$ and $F(x,y) = x\cdot y$. Then we find $r_n = (b(n) \bmod 2)$. This can be generalized to functions that are given by the parity of blocks of the form "$111\cdots11$" for fixed length of the block [13].

Digital sequences are regular sequences [5]. Consequently we find that digital sequences modulo m' are automatic sequences [1, Corollary 16.1.6], which implies some interesting properties. For a detailed treatment of automatic sequences, see [1].

We define the *subword complexity* of a sequence $\mathbf{a}$ that takes only finitely many different values to be

$$p_{\mathbf{a}}(n) = \#\{(a_i,\dots,a_{i+n-1}) : i \geq 0\}.$$

It is well known that the subword complexity of automatic sequences is sub-linear (see [1, Corollary 10.3.2]), *i.e.*, for every automatic sequence $\mathbf{a}$ we have $p_{\mathbf{a}}(n) = O(n)$. For a random sequence $\mathbf{u} \in \{0,1\}^{\mathbb{N}}$, one finds that $p_{\mathbf{u}}(n) = 2^n$ with probability one. Thus, automatic sequences are far from being random.

1.2 Main Result

It is well known that these properties are preserved when considering arithmetic subsequences of automatic sequences and, therefore, digital sequences modulo m'. However, the situation changes completely when one considers the subsequence along squares.

Definition 1.3 A sequence $\mathbf{u} \in \{0,\dots,m'-1\}^{\mathbb{N}}$ is *normal* if, for any $k \in \mathbb{N}$ and any $(c_0,\dots,c_{k-1}) \in \{0,\dots,m'-1\}^k$, we have

$$\lim_{N\to\infty} \frac{1}{N} \#\{i < N : u(i) = c_0,\dots,u(i+k-1) = c_{k-1}\} = (m')^{-k}.$$

https://doi.org/10.4153/CJM-2017-053-1 Published online by Cambridge University Press

Drmota, Mauduit and Rivat showed a first example for that phenomenon [6]. They considered the classical Thue–Morse sequence $(t_n)_{n\geq 0}$ and showed, not only that

$$p_{(t_{n^2})_{n\geq 0}}(k) = 2^k,$$

but also that $(t_{n^2})_{n\geq 0}$ is normal. The fact that $p_{(t_{n^2})_{n\geq 0}}(k) = 2^k$ had already been proved by Moshe [15], who was able to give exponentially growing lower bounds for extractions of the Thue–Morse sequence along polynomials of degree at least 2. In this paper we go one step further than Drmota, Mauduit and Rivat and show a similar result for general digital sequences.

Theorem 1.4 *Let b be a digital function and $m' \in \mathbb{N}$ with* $\gcd(q-1, m') = 1$ *and* $\gcd(m', \gcd(\{b(n) : n \in \mathbb{N}\})) = 1$. *Then $(b(n^2) \bmod m')_{n\in\mathbb{N}}$ is normal.*

There are only few known explicit constructions of normal numbers in a given base [4, Chapters 4 and 5]. This result provides us with a whole class of normal sequences for any given base that can be generated efficiently, *i.e.*, it takes $O(n \log n)$ elementary operations to produce the first n elements.

The easiest construction for normal sequences is the Champernowne construction, which is given by concatenating the base b expansion of successive integers. For example, for base 10 this gives $123456789101112131415\cdots$. Using the first n' integers takes $O(n' \log(n'))$ elementary operations and gives a sequence of length $\Theta(n' \log(n'))$.

Scheerer [17] analyzed the runtime of some algorithms that produce absolutely normal numbers, *i.e.*, real numbers in $[0,1]$ whose expansion in base b is normal for every base b. Algorithms by Sierpinski [19] and Turing [20] use double exponentially many operations and algorithms by Levin [11] and Schmidt [18] use exponentially many operations. Moreover, Becher, Heiber and Slaman [2] gave an algorithm that takes just above n^2 operations to produce the first n digits.

Digital sequences modulo m' have interesting (dynamical) properties. First, they are primitive and, therefore, uniformly recurrent [1, Theorem 10.9.5] , *i.e.*, every block that occurs in the sequence at least once, occurs infinitely often with bounded gaps.

There is a natural way to associate a dynamical system (the symbolic dynamical system) with a sequence that takes only finitely many values.

Definition 1.5 The symbolic dynamical system associated with a sequence $\mathbf{u} \in \{0,\dots,m'-1\}^{\mathbb{N}}$ is the system $(X(\mathbf{u}), T)$, where T is the shift on $\{0,\dots,m'-1\}^{\mathbb{N}}$ and $X(\mathbf{u})$ the closure of the orbit of $\mathbf{u}$ under the action of T for the product topology of $\{0,\dots,m'-1\}^{\mathbb{N}}$.

Some of the mentioned properties of automatic sequences also imply important properties for the associated symbolic dynamical system.

The fact that every digital sequence modulo m', denoted by $\mathbf{u}$, is uniformly recurrent implies that the associated symbolic dynamical system is minimal, *i.e.*, the only closed T invariant sets in $X(\mathbf{u})$ are $\varnothing$ and $X(\mathbf{u})$ [8,16].

Furthermore, the entropy of the symbolic dynamical system associated with sequence $\mathbf{u}$, which takes only finitely many values, is equal to $\lim_{n\to\infty} \log(p_{\mathbf{u}}(n))/n$

([10] or [7]). Consequently, we know that the entropy of the symbolic dynamical system associated with a digital sequence modulo m' equals 0, and therefore, the dynamical system is deterministic.

1.3 Outline of the Proof

In order to prove our main result, we will work with exponential sums. We present here the main theorem on exponential sums and further show its connection to Theorem 1.4.

Theorem 1.6 *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*

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

Lemma 1.7 *Theorem 1.6 implies Theorem 1.4.*

Proof Let $(c_0, \dots, c_{k-1}) \in \{0, \dots, m'-1\}^k$ be an arbitrary sequence of length k. We count the number of occurrences of this sequence in $(b(n^2) \bmod m')_{n\leq N}$. 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,

$$\begin{aligned}
&\Big|\{n < N : (b(n^2) \bmod m', \dots, b((n+k-1)^2) \bmod m') = (c_0, \dots, c_{k-1})\}\Big| \\
&= \sum_{n<N} \mathbf{1}_{[b(n^2)\equiv c_0 \bmod m']} \cdots \mathbf{1}_{[b((n+k-1)^2)\equiv c_{k-1} \bmod m']} \\
&= \sum_{n<N} \prod_{\ell=0}^{k-1} \frac{1}{m'} \sum_{\alpha'_\ell=0}^{m'-1} \mathrm{e}\Big(\frac{\alpha'_\ell}{m'}\big(b((n+\ell)^2) - c_\ell\big)\Big) \\
&= \frac{1}{(m')^k} \sum_{\substack{(\alpha'_0,\dots,\alpha'_{k-1}) \\ \in\{0,\dots,m'-1\}^k}} \mathrm{e}\Big(-\frac{\alpha'_0 c_0 + \cdots + \alpha'_{k-1}c_{k-1}}{m'}\Big) \sum_{n<N} \mathrm{e}\Big(\sum_{\ell=0}^{k-1} \underbrace{\frac{\alpha'_\ell}{m'}}_{=:\alpha_\ell} b((n+\ell)^2)\Big) \\
&= \frac{N}{(m')^k} + \mathcal{O}(N^{1-\eta})
\end{aligned}$$

with the same $\eta > 0$ as in Theorem 1.6. To obtain the last equality we separate the term with $(\alpha'_0, \dots, \alpha'_{k-1}) = (0, \dots, 0)$. ∎

The structure of the rest of the paper is presented next. In Section 2 we discuss some properties of digital sequences. These properties will be very important for the estimates of the Fourier terms. In Section 3, we derive the main ingredients of the proof of Theorem 1.6, which are upper bounds on the Fourier terms

$$H_\lambda^I(h,d) = \frac{1}{q^\lambda} \sum_{0\leq u<q^\lambda} \mathrm{e}\Big(\sum_{\ell=0}^{k-1} \alpha_\ell b_\lambda(u + \ell d + i_\ell) - hq^{-\lambda}\Big),$$

where $I = (i_0, \dots, i_{k-1}) \in \mathbb{N}^k$ with some special properties defined in Section 3.2 and b_λ is a truncated version of b which is properly defined in Definition 2.1.

The main results of Section 3: Proposition 3.7 yields a bound on averages of Fourier transforms and Proposition 3.8 yields a uniform bound on Fourier transforms.

In Section 4, we discuss how Proposition 3.7 and Proposition 3.8 are used to prove Theorem 1.6. The approach is very similar to [6] and we will mainly describe how it must be adapted. We use Van der Corput-like inequalities in order to reduce our problem to sums depending only on few digits of $n^2, (n+1)^2, \dots, (n+k-1)^2$. By detecting these few digits, we are able to remove the quadratic 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 which are dealt with using the results from Section 5.2.

The Fourier terms $H_\lambda^I(h,d)$ appear in the second sum and Propositions 3.7 and 3.8 provide the necessary bounds.

We must distinguish the cases $K = \alpha_0 + \cdots + \alpha_{k-1} \in \mathbb{Z}$ and $K \notin \mathbb{Z}$. Sections 4.1 and 4.2 each tackle one of these cases. In Section 4.1, we prove that, if $K \in \mathbb{Z}$, we deduce Theorem 1.6 from Proposition 3.7. For $K \notin \mathbb{Z}$, Section 4.2 shows that we can deduce Theorem 1.6 from Proposition 3.8.

In Section 5, we present some auxiliary results also used in [6].

2 Digital Functions

In this section we discuss some important properties of digital functions. We start with some basic definitions.

Definition 2.1 We define for $0 \le \mu \le \lambda$ the truncated function b_λ and the two-fold restricted function $b_{\mu,\lambda}$ by

$$b_\lambda(n) = \sum_{j<\lambda} F(\varepsilon_{j+m-1}(n), \dots, \varepsilon_j(n)) \quad \text{and} \quad b_{\mu,\lambda}(n) = b_\lambda(n) - b_\mu(n).$$

We see directly that $b_\lambda(\cdot)\colon \mathbb{N} \to \mathbb{N}$ is a $q^{\lambda+m-1}$ periodic function and we extend it to a ($q^{\lambda+m-1}$ periodic) function $\mathbb{Z} \to \mathbb{N}$ that we also denote by $b_\lambda(\cdot)\colon \mathbb{Z} \to \mathbb{N}$.

For any $n \in \mathbb{N}$, we define $F(n) := F(\varepsilon_{m-1}(n), \dots, \varepsilon_0(n))$. Since $F(0) = 0$, we can rewrite $b(n)$ and $b_\lambda(n)$ for $\lambda \ge 1$ as follows

$$b(n) = \sum_{j\ge 0} F\Big(\Big\lfloor \frac{q^{m-1}n}{q^j} \Big\rfloor\Big), \quad b_\lambda(n) = \sum_{j=0}^{\lambda+m-2} F\Big(\Big\lfloor \frac{q^{m-1}n}{q^j} \Big\rfloor\Big).$$

We show that for any block-additive function, we can choose F without loss of generality such that it fulfills a nice property.

Lemma 2.2 *Let $b\colon \mathbb{N} \to \mathbb{N}$ be a strongly block-additive function corresponding to F'. Then there exists another function F such that b also corresponds to F and*

$$\sum_{j=1}^{m-1} F(nq^j) = 0 \tag{2.1}$$

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

Proof We start by defining a new function $G(n) := \sum_{j=1}^{m-1} F'(nq^j)$. This already allows us to define the function F: $F(n) := F'(n) + G(n) - G(\lfloor n/q \rfloor)$.

https://doi.org/10.4153/CJM-2017-053-1 Published online by Cambridge University Press

We find directly that $G(0) = F(0) = 0$. It remains to show that b corresponds to F and that (2.1) holds, which are simple computations,

$$\begin{aligned}\sum_{j\geq 0} F\Big(\Big\lfloor \frac{q^{m-1}n}{q^j}\Big\rfloor\Big) &= \sum_{j\geq 0} F'\Big(\Big\lfloor \frac{q^{m-1}n}{q^j}\Big\rfloor\Big) + \sum_{j\geq 0} G\Big(\Big\lfloor \frac{q^{m-1}n}{q^j}\Big\rfloor\Big) - \sum_{j\geq 0} G\Big(\Big\lfloor \frac{q^{m-1}n}{q^{j+1}}\Big\rfloor\Big)\\ &= b(n) + G(0) = b(n).\end{aligned}$$

Furthermore, we find

$$\begin{aligned}\sum_{j=1}^{m-1} F(nq^j) &= \sum_{j=1}^{m-1} F'(nq^j) + \sum_{j=1}^{m-1} G(nq^j) - \sum_{j=1}^{m-1} G(nq^{j-1})\\ &= \sum_{j=1}^{m-1} F'(nq^j) + G(nq^{m-1}) - G(n)\\ &= \sum_{j=1}^{m-1} F'(nq^j) + 0 - \sum_{j=1}^{m-1} F'(nq^j) = 0.\end{aligned}$$ ∎

Henceforth, we assume that (2.1) holds for any strongly block-additive function b. This allows us to find an easier expression for b.

Corollary 2.3 *Let $b(n)$ be a digital function fulfilling* (2.1). *Then*

$$b(n) = \sum_{j\geq 0} F\Big(\Big\lfloor \frac{n}{q^j}\Big\rfloor\Big), \quad b_\lambda(n) = \sum_{j=0}^{\lambda-1} F\Big(\Big\lfloor \frac{n}{q^j}\Big\rfloor\Big)$$

holds for all $n, \lambda \in \mathbb{N}$.

We easily find the following recursion.

Lemma 2.4 *Let $\alpha \in \mathbb{N}$, $n_1 \in \mathbb{N}$, and $0 \leq n_2 < q^\alpha$. Then*

$$b_\lambda(n_1 q^\alpha + n_2) = b_{\lambda-\alpha}(n_1) + b_\alpha(n_1 q^\alpha + n_2) \tag{2.2}$$

holds for all $\lambda > \alpha$ and $b(n_1 q^\alpha + n_2) = b(n_1) + b_\alpha(n_1 q^\alpha + n_2)$.

Proof We compute $b_\lambda(n_1 q^\alpha + n_2)$:

$$\begin{aligned}b_\lambda(n_1 q^\alpha + n_2) &= \sum_{j=0}^{\lambda-1} F\Big(\Big\lfloor \frac{n_1 q^\alpha + n_2}{q^j}\Big\rfloor\Big)\\ &= \sum_{j=\alpha}^{\lambda-1} F\Big(\Big\lfloor \frac{n_1 q^\alpha + n_2}{q^j}\Big\rfloor\Big) + \sum_{j=0}^{\alpha-1} F\Big(\Big\lfloor \frac{n_1 q^\alpha + n_2}{q^j}\Big\rfloor\Big)\\ &= \sum_{j=0}^{\lambda-\alpha-1} F\Big(\Big\lfloor \frac{n_1}{q^j}\Big\rfloor\Big) + \sum_{j=0}^{\alpha-1} F\Big(\Big\lfloor \frac{n_1 q^\alpha + n_2}{q^j}\Big\rfloor\Big)\\ &= b_{\lambda-\alpha}(n_1) + b_\alpha(n_1 q^\alpha + n_2).\end{aligned}$$

The second case can be treated analogously. ∎

As we are dealing with the distribution of digital functions along a special subsequence, we will start discussing some distributional results for digital functions.

Lemma 2.5 *Let b be a strongly block-additive function and $m' > 1$. Then the following three statements are equivalent.*

(i) *There exists $n \in \mathbb{N}$ such that $m' \nmid b(n)$.*
(ii) *There exists $n < q^m$ such that $m' \nmid F(n)$.*
(iii) *There exists $n < q^m$ such that $m' \nmid b(n)$.*

Proof Obviously (iii) $\Rightarrow$ (i).

Next we show that (i) $\Rightarrow$ (ii). Let n_0 be the smallest natural number > 0 such that $m' \nmid b(n_0)$. By Lemma 2.4, $b(n_0) = b(\lfloor n_0/q \rfloor) + F(n_0)$ holds. By the definition of n_0, we have $m' \mid b(\lfloor n_0/q \rfloor)$, and therefore, $m' \nmid F(n_0) = F(n_0 \bmod q^m)$.

It remains to prove that (ii) $\Rightarrow$ (iii). Let n_0 be the smallest natural number > 0 such that $m' \nmid F(n_0)$. By (ii), we have $n_0 < q^m$. We compute $b(n_0) \bmod m'$,

$$b(n_0) = \sum_{j \geq 0} F\Big(\Big\lfloor \frac{n_0}{q^j} \Big\rfloor \Big) \equiv F(n_0) \not\equiv 0 \pmod{m'}$$

as $\lfloor \frac{n_0}{q^j} \rfloor < n_0$ for $j \geq 1$ implies that $F\big(\lfloor \frac{n_0}{q^j} \rfloor \big) \equiv 0 \pmod{m'}$. ∎

Remark 2.6 The following example shows that in Lemma 2.5, we cannot replace $m' \nmid \cdot$ by $\gcd(m', \cdot) = 1$. Let $m = 1, q = 3, m' = 6$ and $F(0) = 0, F(1) = 2, F(2) = 3$. We see that $\gcd(m', F(n)) > 1$ for all $n < q^m = 3$ and also $\gcd(m', b(n)) > 1$ for all $n < q^m = 3$. However, $b(5) = F(1) + F(2) = 5$ and $\gcd(m', b(5)) = 1$.

Next, we show a technical result concerning block-additive functions that will be useful later on.

Lemma 2.7 *Let b be a strongly block-additive function in base q and $k > 1$ such that $\gcd(k, q-1) = 1$ and $\gcd(k, \gcd(\{b(n) : n \in \mathbb{N}\})) = 1$. Then there exist integers $\mathbf{e}_1, \mathbf{e}_2 < q^{2m-1}$ such that*

$$b(q^{m-1}(\mathbf{e}_1+1)-1) - b(q^{m-1}(\mathbf{e}_1+1)) \not\equiv b(q^{m-1}(\mathbf{e}_2+1)-1) - b(q^{m-1}(\mathbf{e}_2+1)) \pmod k$$

holds.

Proof Without loss of generality we can restrict ourselves to the case $p \in \mathbb{P}$ where $p \mid k$. Let us assume on the contrary that there exists c such that

$$b(q^{m-1}(\mathbf{e}+1)-1) - b(q^{m-1}(\mathbf{e}+1)) \equiv c \pmod p$$

holds for all $\mathbf{e} < q^{2m-1}$. Under this assumption, we find a new expression for $b(n) \bmod p$, where $n < q^m$:

$$\begin{aligned} n \cdot q^{m-1} c &\equiv \sum_{\mathbf{e} < n q^{m-1}} \big(b(q^{m-1}(\mathbf{e}+1)-1) - b(q^{m-1}(\mathbf{e}+1)) \big) \\ &\equiv \sum_{\mathbf{e} < n q^{m-1}} \big(b(\mathbf{e}) + b_{m-1}(q^{m-1}\mathbf{e} + q^{m-1} - 1) - b(\mathbf{e}+1) \big) \\ &\equiv -b(nq^{m-1}) + \sum_{\mathbf{e} < n q^{m-1}} b_{m-1}(q^{m-1}\mathbf{e} + q^{m-1} - 1) \\ &\equiv -b(nq^{m-1}) + n \sum_{\mathbf{e} < q^{m-1}} b_{m-1}(q^{m-1}\mathbf{e} + q^{m-1} - 1). \end{aligned}$$

The last equality holds since $b_{m-1}(q^{m-1}\mathbf{e}+q^{m-1}-1)$ is a q^{m-1} periodic function in $\mathbf{e}$. This gives

$$b(n)=b(nq^{m-1})\equiv n\Big(\sum_{\mathbf{e}<q^{m-1}} b_{m-1}(q^{m-1}\mathbf{e}+q^{m-1}-1)-q^{m-1}c\Big)\,(\mathrm{mod}\,p). \tag{2.3}$$

By comparing this expression for $b(1)$ and $b(q)$ (note that $b(1)=b(q)$), we find

$$(q-1)\Big(\sum_{\mathbf{e}<q^{m-1}} b_{m-1}(q^{m-1}\mathbf{e}+q^{m-1}-1)-q^{m-1}c\Big)\equiv 0 \pmod p$$
$$\sum_{\mathbf{e}<q^{m-1}} b_{m-1}(q^{m-1}\mathbf{e}+q^{m-1}-1)-q^{m-1}c\equiv 0 \pmod p$$

as $\gcd(p,q-1)=1$.

Together with (2.3), this implies that $p\mid b(n)$ for all $n<q^m$. By Lemma 2.5, this is a contradiction to $\gcd(p,\gcd(\{b(n):n\in\mathbb{N}\}))=1$. ■

We will use this result in a different form.

Corollary 2.8 *Let b be a strongly block-additive function in base q and let $m'>1$ such that $\gcd(m',q-1)=1$ and $\gcd(m',\gcd(\{b(n):n\in\mathbb{N}\}))=1$. For every $\alpha\in\{\frac{1}{m'},\dots,\frac{m'-1}{m'}\}$ there exist $\mathbf{e}_1,\mathbf{e}_2<q^{2m-1}$ and $d\in\mathbb{N}$ such that $d\alpha\notin\mathbb{Z}$ and*

$$b(q^{m-1}(\mathbf{e}_1+1)-1)-b(q^{m-1}(\mathbf{e}_1+1))-b(q^{m-1}(\mathbf{e}_2+1)-1)+b(q^{m-1}(\mathbf{e}_2+1))=d.$$

Proof Let $\alpha=x/y$ where $\gcd(x,y)=1$ and $1<y\mid m'$. We apply Lemma 2.7 for $k=y$ and find $\mathbf{e}_1,\mathbf{e}_2$ such that

$$b(q^{m-1}(\mathbf{e}_1+1)-1)-b(q^{m-1}(\mathbf{e}_1+1))-b(q^{m-1}(\mathbf{e}_2+1)-1)+b(q^{m-1}(\mathbf{e}_2+1))=d,$$

where $d\not\equiv 0 \pmod y$. This implies $d\alpha=\frac{dx}{y}\not\equiv 0 \pmod 1$. ■

3 Bounds on Fourier Transforms

The goal of this section is to prove Propositions 3.7 and 3.8. To find the necessary bounds we first need to recall one important result on the norm of matrix products that was first presented by Drmota, Mauduit, and Rivat [6]. Then we deal with Fourier estimates and formulate Propositions 3.7 and 3.8. Sections 3.3 and 3.4 give proofs of Propositions 3.7 and 3.8, respectively.

3.1 Auxiliary Results for the Bounds of the Fourier Transforms

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

Lemma 3.1 *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 $\sum_{j=1}^{N}|M_{\ell;i,j}|\le 1$, 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 the following hold.*

(i) *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*

$$|A_{i,1}| \geq c_0 \quad \text{or} \quad \sum_{j=1}^{N} |A_{i,j}| \leq 1 - \eta \quad \text{for every row } i. \tag{3.1}$$

(ii) *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*

$$\sum_{j=1}^{N} |B_{1,j}| \leq 1 - \eta. \tag{3.2}$$

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

$$\Big\| \prod_{\ell=r}^{r+k-1} \mathbf{M}_\ell \Big\|_\infty \leq C q^{-\delta k}$$

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

Proof See [6]. ∎

Lemma 3.2 *Let* $x_1, x_2, \xi_1, \xi_2 \in \mathbb{R}$. *Then*

$$|\,\mathrm{e}(x_1) + \mathrm{e}(x_1 + \xi_1)| + |\,\mathrm{e}(x_2) + \mathrm{e}(x_2 + \xi_2)| \leq 4 - 8\Big(\sin\Big(\frac{\pi\|\xi_1 - \xi_2\|}{4}\Big)\Big)^2.$$

Proof The proof is a straightforward computation and can be found at the end of the proof of [13, Lemma 12]. ∎

3.2 Fourier Estimates

In this section, we discuss some general properties of the occurring Fourier terms. 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 $i_0 < q^{m-1}$ and $i_{\ell-1} \leq i_\ell \leq i_{\ell-1} + q^{m-1}$ for $1 \leq \ell \leq k-1$. Furthermore, we denote by $\mathcal{I}'_k$ the set of integer vectors $I' = (i'_0, \dots, i'_{k-1})$ with $i'_0 = 0$ and $i'_{\ell-1} \leq i'_\ell \leq i'_{\ell-1} + 1$. This set $\mathcal{I}_k$ obviously consists of $q^{m-1}(q^{m-1}+1)^{k-1}$ elements. For any $I \in \mathcal{I}'_k$, $h \in \mathbb{Z}$ and $(d, \lambda) \in \mathbb{N}^2$, we define

$$H^I_\lambda(h,d) = \frac{1}{q^{\lambda+m-1}} \sum_{0 \leq u < q^{\lambda+m-1}} \mathrm{e}\Big(\sum_{\ell=0}^{k-1} \alpha_\ell b_\lambda(u + \ell d + i_\ell) - huq^{-\lambda-m+1}\Big),$$

for fixed coefficients $\alpha_\ell \in \{\frac{0}{m'}, \dots, \frac{m'-1}{m'}\}$. The sum $H^I_\lambda(\cdot, d)$ can then be seen as the discrete Fourier transform of the function $u \mapsto \mathrm{e}\big(\sum_{\ell=0}^{k-1} \alpha_\ell b_\lambda(u + \ell d + i_\ell)\big)$, which is $q^{\lambda+m-1}$ periodic.

Furthermore, we define the important parameter $K := \alpha_0 + \cdots + \alpha_{k-1}$.

We would like to find a simple recursion for H_λ in terms of $H_{\lambda-1}$. Instead we relate it to a different function for which the recursion is much simpler,

$$G^I_\lambda(h,d) = \frac{1}{q^\lambda} \sum_{u < q^\lambda} \mathrm{e}\Big(\sum_{\ell=0}^{k-1} \alpha_\ell b_\lambda(q^{m-1}(u + \ell d) + i_\ell) - huq^{-\lambda}\Big).$$

https://doi.org/10.4153/CJM-2017-053-1 Published online by Cambridge University Press

This sum $G_\lambda^I(\,.\,,d)$ can then be seen as the discrete Fourier transform of the function $u \mapsto \mathrm{e}\big(\sum_{\ell=0}^{k-1} \alpha_\ell b_\lambda(q^{m-1}(u+\ell d)+i_\ell)\big)$, which is q^λ periodic. We show now how G and H are related.

Lemma 3.3 *Let $I \in \mathcal{I}'_k$, $h \in \mathbb{Z}$, $(d,\lambda) \in \mathbb{N}^2$ and $\delta \in \{0,\dots,q^{m-1}-1\}$. It holds*

$$H_\lambda^I(h, q^{m-1}d+\delta) = \frac{1}{q^{m-1}} \sum_{\varepsilon=0}^{q^{m-1}-1} \mathrm{e}\Big(-\frac{h\varepsilon}{q^{\lambda+m-1}}\Big)\, \mathrm{G}_\lambda^{J_{\varepsilon,\delta}}(h,d), \tag{3.3}$$

where $J_{\varepsilon,\delta} = J_{\varepsilon,\delta}(I) = (i_\ell + \ell\delta + \varepsilon)_{\ell \in \{0,\dots,k-1\}} \in \mathcal{I}_k$.

Proof One checks easily that $J_{\varepsilon,\delta}(I) \in \mathcal{I}_k$. We evaluate $H_\lambda^I(h, q^{m-1}d+\delta)$.

$$\begin{aligned}
&H_\lambda^I(h, q^{m-1}d+\delta)\\
&\quad= \frac{1}{q^{\lambda+m-1}} \sum_{0\le u<q^{\lambda+m-1}} \mathrm{e}\Big(\sum_{\ell=0}^{k-1} \alpha_\ell b_\lambda(u+\ell(q^{m-1}d+\delta)+i_\ell) - huq^{-\lambda-m+1}\Big)\\
&\quad= \frac{1}{q^{\lambda+m-1}} \sum_{\varepsilon<q^{m-1}} \sum_{0\le u<q^\lambda} \mathrm{e}\Big(-\frac{h(q^{m-1}u)}{q^{\lambda+m-1}}\Big)\, \mathrm{e}\Big(-\frac{h\varepsilon}{q^{\lambda+m-1}}\Big)\\
&\qquad\quad \times \mathrm{e}\Big(\sum_{\ell=0}^{k-1} \alpha_\ell b_\lambda(q^{m-1}u+\varepsilon+\ell(q^{m-1}d+\delta)+i_\ell)\Big)\\
&\quad= \frac{1}{q^{\lambda+m-1}} \sum_{\varepsilon<q^{m-1}} \sum_{u<q^\lambda} \mathrm{e}\big(-\frac{hu}{q^\lambda}\big)\, \mathrm{e}\Big(-\frac{h\varepsilon}{q^{\lambda+m-1}}\Big)\\
&\qquad\quad \times \mathrm{e}\Big(\sum_{\ell=0}^{k-1} \alpha_\ell b_\lambda((u+\ell d)q^{m-1} + (\ell\delta+i_\ell+\varepsilon))\Big)\\
&\quad= \frac{1}{q^{m-1}} \sum_{\varepsilon<q^{m-1}} \mathrm{e}\Big(-\frac{h\varepsilon}{q^{\lambda+m-1}}\Big)\, \mathrm{G}_\lambda^{J_{\varepsilon,\delta}}(h,d).
\end{aligned}$$

∎

Next we define a transformation on $\mathcal{I}_k$ and a weight function ν.

Definition 3.4 Let $j \ge 1$ and $\varepsilon,\delta \in \{0,\dots,q^j-1\}$. Then we define for $I \in \mathcal{I}_k$

$$\begin{aligned}
T_{\varepsilon,\delta}^j(I) &:= \Big(\Big\lfloor \frac{i_\ell + q^{m-1}(\varepsilon+\ell\delta)}{q^j}\Big\rfloor\Big)_{\ell\in\{0,\dots,k-1\}}\\
\nu^j(I,\varepsilon,\delta) &:= \mathrm{e}\Big(\sum_{\ell<k} \alpha_\ell \cdot b_j\big(i_\ell + q^{m-1}(\varepsilon+\ell\delta)\big)\Big).
\end{aligned}$$

We see immediately that $|\nu^j(I,\varepsilon,\delta)| = 1$ for all possible values of j, I, ε and δ. Furthermore, we extend the definition of T^j for arbitrary ε,δ by

$$T_{\varepsilon,\delta}^j(I) := T^j_{\varepsilon \bmod q^j, \delta \bmod q^j}(I).$$

The next lemma shows some basic properties of these functions.

https://doi.org/10.4153/CJM-2017-053-1 Published online by Cambridge University Press

Lemma 3.5 *Let $\lambda, j, j_1, j_2 \in \mathbb{N}$, $\varepsilon, \delta \in \{0, \dots, q^j - 1\}$, and $\varepsilon_i, \delta_i \in \{0, \dots, q^{j_i} - 1\}$. Then the following facts hold.*

(i) $T^j_{\varepsilon,\delta}(I) \in \mathcal{I}_k$.

(ii) $T^{j_2}_{\varepsilon_2,\delta_2} \circ T^{j_1}_{\varepsilon_1,\delta_1} = T^{j_1+j_2}_{\varepsilon_2 q^{j_1}+\varepsilon_1, \delta_2 q^{j_1}+\delta_1}$.

(iii) $G^I_\lambda(h,d) = \frac{1}{q^\lambda}\sum_{u<q^\lambda} \nu^\lambda(I,u,d)\,\mathrm{e}(-huq^{-\lambda})$.

Proof (i) and (ii) are direct consequences of basic properties of the floor function and (iii) is just a reformulation of the definition of G in terms of ν. ■

Now we can find a nice recursion for the Fourier transform G.

Lemma 3.6 *Let $I \in \mathcal{I}_k$, $h \in \mathbb{Z}$, $d, \lambda \in \mathbb{N}$ and $1 \le j \le \lambda$, $\delta \in \{0, \dots, q^j - 1\}$. We have*

$$G^I_\lambda(h, q^j d + \delta) = \frac{1}{q^j}\sum_{\varepsilon<q^j} \mathrm{e}(-h\varepsilon q^{-\lambda})\nu^j(I,\varepsilon,\delta)\cdot G^{T^j_{\varepsilon,\delta}(I)}_{\lambda-j}(h,d).$$

Proof We evaluate $G^I_\lambda(h, q^j d + \delta)$ and use (2.2):

$$\begin{aligned}
G^I_\lambda(h, q^j d + \delta) &= \frac{1}{q^\lambda}\sum_{u<q^\lambda} \mathrm{e}\Big(\sum_{\ell=0}^{k-1}\alpha_\ell b_\lambda(q^{m-1}(u+\ell(q^j d+\delta)) + i_\ell) - huq^{-\lambda}\Big)\\
&= \frac{1}{q^j}\sum_{\varepsilon<q^j}\frac{1}{q^{\lambda-j}}\sum_{u<q^{\lambda-j}} \mathrm{e}\Big(\sum_{\ell=0}^{k-1}\alpha_\ell b_\lambda(q^{m-1+j}(u+\ell d) + q^{m-1}(\varepsilon+\ell\delta) + i_\ell)\Big)\\
&\quad\times \mathrm{e}(-h(uq^j+\varepsilon)q^{-\lambda})\\
&= \frac{1}{q^j}\sum_{\varepsilon<q^j}\mathrm{e}\Big(\sum_{\ell=0}^{k-1}\alpha_\ell b_j(q^{m-1}(\varepsilon+\ell\delta)+i_\ell)\Big)\,\mathrm{e}(-h\varepsilon q^{-\lambda})\frac{1}{q^{\lambda-j}}\\
&\quad\times\sum_{u<q^{\lambda-j}}\mathrm{e}\Big(\sum_{\ell=0}^{k-1}\alpha_\ell b_{\lambda-j}\Big(q^{m-1}(u+\ell d) + \Big\lfloor\frac{\varepsilon q^{m-1}+\ell\delta q^{m-1}+i_\ell}{q^j}\Big\rfloor\Big) - huq^{-\lambda+j}\Big)\\
&= \frac{1}{q^j}\sum_{\varepsilon<q^j}\nu^j(I,\varepsilon,\delta)\,\mathrm{e}(-h\varepsilon q^{-\lambda})\cdot G^{T^j_{\varepsilon,\delta}(I)}_{\lambda-j}(h,d).
\end{aligned}$$
■

The following propositions are crucial for our proof of Theorem 1.6.

Proposition 3.7 *If $K \equiv 0 \pmod 1$ and $\frac{1}{2}\lambda \le \lambda' \le \lambda$, then there exists $\eta > 0$ such that for any $I \in \mathcal{I}'_k$ $\frac{1}{q^{\lambda'}}\sum_{0\le d<q^{\lambda'}} |H^I_\lambda(h,d)|^2 \ll q^{-\eta\lambda}$ holds uniformly for all integers h.*

Proposition 3.8 *If $K \not\equiv 0 \pmod 1$, then there exists $\eta > 0$ such that for any $I \in \mathcal{I}'_k$*

$$|H^I_\lambda(h,d)| \ll q^{-\eta L}\max_{J\in\mathcal{I}_k}|G^J_{\lambda-L}(h, \lfloor d/q^L\rfloor)|$$

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

https://doi.org/10.4153/CJM-2017-053-1 Published online by Cambridge University Press

3.3 Proof of Proposition 3.7

We start by reducing the problem from $H_\lambda^I(h,d)$ to $G_\lambda^I(h,d)$ for which we have found a nice recursion.

Proposition 3.9 *For $K \in \mathbb{Z}$ and $\frac{1}{2}\lambda \le \lambda' \le \lambda$, we find $\eta > 0$ such that for any $I \in \mathcal{I}_k$*

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

holds uniformly for all integers h.

Lemma 3.10 *Proposition* 3.9 *implies Proposition* 3.7.

Proof We see by (3.3) that

$$|H_\lambda^I(h,d)|^2 \le \max_{J\in\mathcal{I}_k} |G_\lambda^J(h,\lfloor d/q^{m-1}\rfloor)|^2 \le \sum_{J\in\mathcal{I}_k} |G_\lambda^J(h,\lfloor d/q^{m-1}\rfloor)|^2.$$

Thus we find

$$\frac{1}{q^{\lambda'}} \sum_{0\le d<q^{\lambda'}} |H_\lambda^I(h,d)|^2 \le \sum_{J\in\mathcal{I}_k} \frac{1}{q^{\lambda'}} \sum_{0\le d<q^{\lambda'}} |G_\lambda^J(h,\lfloor d/q^{m-1}\rfloor)|^2 \ll q^{-\eta\lambda}. \qquad \blacksquare$$

Using Lemma 3.6, 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 $\lambda,\lambda' \ge 1$ and $1 \le j \le \min(\lambda,\lambda')$ it yields for $\Phi_{\lambda,\lambda'}^{I,I'}(h)$ the following expression:

$$\frac{1}{q^{3j}} \sum_{\delta<q^j} \sum_{\varepsilon_1<q^j} \sum_{\varepsilon_2<q^j} \mathrm{e}\Big(-\frac{(\varepsilon_1-\varepsilon_2)h}{q^\lambda}\Big) v^j(I,\varepsilon_1,\delta)\overline{v^j(I,\varepsilon_2,\delta)}\Phi_{\lambda-j,\lambda'-j}^{T^j_{\varepsilon_1,\delta}(I),T^j_{\varepsilon_2,\delta}(I')}(h).$$

To find this recursion, one has to split the sum over $0 \le d < q^{\lambda'}$ into the equivalence classes modulo q^j. This identity gives rise to a vector recursion for $\Psi_{\lambda,\lambda'}(h) = (\Phi_{\lambda,\lambda'}^{I,I'}(h))_{(I,I')\in\mathcal{I}_k^2}$. We use the recursion for $j=1$. We have $\Psi_{\lambda,\lambda'}(h) = \mathbf{M}(h/q^\lambda)\cdot\Psi_{\lambda-1,\lambda'-1}(h)$, where the $(q^{m-1}(q^{m-1}+1))^2 \times (q^{m-1}(q^{m-1}+1))^2$ 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 λ and λ'. By construction, all absolute row sums of $\mathbf{M}(\beta)$ are bounded by 1.

It is useful to interpret these matrices as weighted directed graphs. 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 $(\mathrm{T}_{\varepsilon_1,\delta}(I),\mathrm{T}_{\varepsilon_2,\delta}(I'))$, where $(\delta,\varepsilon_1,\varepsilon_2) \in \{0,\dots,q-1\}^3$, with corresponding weights

$$\frac{1}{q^3}\mathrm{e}\Big(-\frac{(\varepsilon_1-\varepsilon_2)h}{q^\lambda}\Big) v^1(I,\varepsilon_1,\delta)\overline{v^1(I',\varepsilon_2,\delta)}.$$

Products of j such matrices correspond to oriented paths of length j in these graphs, which are weighted with the corresponding products. The entries at position

$$((I,I'),(J,J'))$$

https://doi.org/10.4153/CJM-2017-053-1 Published online by Cambridge University Press

of such product matrices correspond to the sum of weights along paths from (I, I') to (J, J'). Lemma 3.6 allows us to describe this product of matrices directly.

Lemma 3.11 *The entry* $((I, I'), (J, J'))$ *of* $\mathbf{M}(h/q^{\lambda})\mathbf{M}(h/q^{\lambda-1})\cdots\mathbf{M}(h/q^{\lambda-j+1})$ *is equal to*

$$\frac{1}{q^{3j}}\sum_{\delta<q^j}\sum_{\varepsilon_1,\varepsilon_2<q^j}\mathbf{1}_{[T^j_{\varepsilon_1,\delta}(I)=J]}\mathbf{1}_{[T^j_{\varepsilon_2,\delta}(I')=J']}\nu^j(I,\varepsilon_1,\delta)\overline{\nu^j(I',\varepsilon_2,\delta)}\,\mathrm{e}\Big(-\frac{(\varepsilon_1-\varepsilon_2)h}{q^{\lambda}}\Big).$$

Proof This follows directly by Lemma 3.6. ∎

This product of matrices corresponds to oriented paths of length j. These can be encoded by the triples $(\varepsilon_1, \varepsilon_2, \delta)$, and they correspond to a path from (I, I') to $(T^j_{\varepsilon_1,\delta}(I), T^j_{\varepsilon_2,\delta}(I'))$ with unimodular weight $\nu^j(I,\varepsilon_1,\delta)\overline{\nu^j(I',\varepsilon_2,\delta)}\,\mathrm{e}\big(-\frac{(\varepsilon_1-\varepsilon_2)h}{q^{\lambda}}\big)$.

To simplify further computations we define

$$n^{(j)}_{(I,I'),(J,J')} := \sum_{\delta<q^j}\sum_{\varepsilon_1,\varepsilon_2<q^j}\mathbf{1}_{[T^j_{\varepsilon_1,\delta}(I)=J]}\mathbf{1}_{[T^j_{\varepsilon_2,\delta}(I')=J']}$$

and find directly that $\sum_{(J,J')\in\mathcal{I}_k^2} n^{(j)}_{(I,I'),(J,J')} = q^{3j}$ and the absolute value of the entry $((I, I'), (J, J'))$ of

$$\mathbf{M}(h/q^{\lambda})\mathbf{M}(h/q^{\lambda-1})\cdots\mathbf{M}(h/q^{\lambda-j+1})$$

is bounded by $n^{(j)}_{(I,I'),(J,J')}q^{-3j}$.

In order to prove Proposition 3.7, we will use Lemma 3.1 uniformly for h with $\mathbf{M}_l = \mathbf{M}(h/q^l)$. Therefore, we need to check (3.1) and (3.2). Note that, since $\frac{1}{2}\lambda \le \lambda' \le \lambda$, 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 3.12 *The matrices M_l defined above fulfill* (3.1) *of Lemma* 3.1.

Proof We need to show that there exists an integer $m_0 \ge 1$ 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 (3.1) of Lemma 3.1. We define $m_0 = m - 1 + \lceil\log_q(k+1)\rceil$. It follows directly from the definition that $T^{m_0}_{0,0}(I) = \mathbf{0}$ for all $I \in \mathcal{I}_k$. In the graph interpretation this means that for every vertex (I, I') there is a path of length m_0 from (I, I') to $(\mathbf{0}, \mathbf{0})$. Fix a row indexed by (I, I') in the matrix $\mathbf{A}$. We already showed that the entry $A_{(I,I'),(\mathbf{0},\mathbf{0})}$ is the sum of at least one term of absolute value q^{-3m_0}, *i.e.*, $n^{(m_0)}_{(I,I'),(\mathbf{0},\mathbf{0})} \ge 1$.

There are two possible cases. If the absolute row sum is at most $\le 1-\eta$ with $\eta \le q^{-3m_0}$ then we are done.

In case the absolute row sum is strictly greater than $1-\eta$, we show that

$$|A_{(I,I'),(\mathbf{0},\mathbf{0})}| \ge q^{-3m_0}/2.$$

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}, *i.e.*, $n^{(m_0)}_{(I,I'),(\mathbf{0},\mathbf{0})} \ge 2$. Thus, we can use the triangle inequality to bound the absolute row sum by

$$\sum_{(J,J')} |A_{(I,I'),(J,J')}| \le |A_{(I,I'),(\mathbf{0},\mathbf{0})}| + q^{-3m_0} \sum_{(J,J')\ne(\mathbf{0},\mathbf{0})} n^{(m_0)}_{(I,I'),(J,J')}.$$

Since $\sum_{(J,J')} n^{(m_0)}_{(I,I'),(J,J')} = q^{3m_0}$, we find

$$\begin{aligned}\sum_{(J,J')} |A_{(I,I'),(J,J')}| &\le |A_{(I,I'),(\mathbf{0},\mathbf{0})}| + 1 - q^{-3m_0} n^{(m_0)}_{(I,I'),(\mathbf{0},\mathbf{0})}\\ &\le q^{-3m_0}/2 + 1 - 2q^{-3m_0} < 1 - q^{-3m_0}.\end{aligned}$$

This contradicts the assumption that the absolute row sum is strictly greater than $1-\eta \ge 1-q^{-3m_0}$. Consequently, we find $|A_{(I,I'),(\mathbf{0},\mathbf{0})}| \ge c_0$ for $c_0 = q^{-3m_0}/2$. ∎

Lemma 3.13 *The matrices M_l fulfill* (3.2) *of Lemma* 3.1.

Proof We need to show that there exists an integer $m_1 \ge 1$ 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 row-sum 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 $T_{00}^{m+\lfloor\log_q(k)\rfloor}(\mathbf{0}) = T_{10}^{m+\lfloor\log_q(k)\rfloor}(\mathbf{0}) = \mathbf{0}$, 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 $k_0 = k_0(m_1) \ge 2$ terms of absolute value q^{-3m_1}, for every $m_1 \ge m + \lfloor\log_q(k)\rfloor$. This means that there are $k_0 \ge 2$ paths from $(\mathbf{0},\mathbf{0})$ to $(\mathbf{0},\mathbf{0})$ of length m_1 in the corresponding graph, or in other words, $n^{m_1}_{(\mathbf{0},\mathbf{0}),(\mathbf{0},\mathbf{0})} = k_0(m_1) \ge 2$.

Our goal is to construct two paths $(\varepsilon_1^i, \varepsilon_2^i, \delta^i)$ from $(\mathbf{0},\mathbf{0})$ to $(\mathbf{0},\mathbf{0})$ such that

$$\Big|\sum_{i=1}^{2} v^{m_1}(\mathbf{0},\varepsilon_1^i,\delta^i)\overline{v^{m_1}(\mathbf{0},\varepsilon_2^i,\delta^i)}\,\mathrm{e}\Big(-\frac{(\varepsilon_1^i-\varepsilon_2^i)h}{q^\lambda}\Big)\Big| \le 2-\eta$$

holds for all $h \in \mathbb{Z}$.

We construct a path from $\mathbf{0}$ to $(q^{m-1}-1,\dots,q^{m-1}-1,q^{m-1},\dots,q^{m-1}) =: I_0 \in \mathcal{I}_k$ with exactly n_0+1 times $q^{m-1}-1$, where $n_0 = \min\{n\in\mathbb{N} : \alpha_n \ne 0\}$. We set $n_1 = \lfloor\log_q(k)\rfloor + m$ and have the following lemma.

Lemma 3.14 *Let n_0, n_1, and I_0 be as above. Then $T^{n_1}_{q^{n_1}-n_0-1,1}(\mathbf{0}) = I_0$.*

Proof This follows directly by the definitions and simple computations. ∎

Applying Lemma 3.14, we obtain a transformation from $\mathbf{0}$ to I_0. Applying this transformation component-wise gives a path from $(\mathbf{0},\mathbf{0})$ to (I_0,I_0). We concatenate this path with another path $(\mathbf{e}_1,\mathbf{e}_2,0)$ of length $n_2 = 3m-1$ where $\mathbf{e}_i < q^{2m-1}$. The weight of the concatenation of these two paths equals

$$\begin{aligned}&\nu^{n_1}(\mathbf{0}, q^{n_1}-n_0-1,1)\nu^{n_2}(I_0,\mathbf{e}_1,0)\\&\qquad\times\overline{\nu^{n_1}(\mathbf{0}, q^{n_1}-n_0-1,1)\nu^{n_2}(I_0,\mathbf{e}_2,0)}\,\mathrm{e}\Big(-\frac{(\mathbf{e}_1-\mathbf{e}_2)h}{q^{\lambda-n_1}}\Big)\\&\qquad\qquad=\nu^{n_2}(I_0,\mathbf{e}_1,0)\overline{\nu^{n_2}(I_0,\mathbf{e}_2,0)}\,\mathrm{e}\Big(-\frac{(\mathbf{e}_1-\mathbf{e}_2)h}{q^{\lambda-n_1}}\Big).\end{aligned}$$

We denote by $I_{0|\ell}$ the ℓ-th coordinate of I_0 and see that

$$\begin{aligned}T^{3m-1}_{\mathbf{e}_i,0}(I_0)&=\Big(\Big\lfloor\frac{I_{0|\ell}+q^{m-1}\mathbf{e}_i}{q^{3m-1}}\Big\rfloor\Big)_{\ell\in\{0\cdots k-1\}}\le\Big(\Big\lfloor\frac{q^{m-1}+q^{m-1}(q^{2m-1}-1)}{q^{3m-1}}\Big\rfloor\Big)_{\ell\in\{0\cdots k-1\}}\\&=\Big(\Big\lfloor\frac{q^{m-1}\cdot q^{2m-1}}{q^{3m-1}}\Big\rfloor\Big)_{\ell\in\{0\cdots k-1\}}=\mathbf{0}\end{aligned}$$

Thus, we have found a path from $(\mathbf{0},\mathbf{0})$ to $(\mathbf{0},\mathbf{0})$ for each $\mathbf{e}_2<q^{2m-1}$.

We can use the special structure of I_0 to make the weight of this path more explicit. First, we note that $\sum_{\ell=0}^{n_0}\alpha_\ell=\alpha_{n_0}$ by the definition of n_0. Furthermore, we use the condition $K=\sum_\ell\alpha_\ell\in\mathbb{Z}$ to find $\sum_{\ell=n_0+1}^{k-1}\alpha_\ell\equiv-\alpha_{n_0}\pmod 1$.

We find by the definition of ν that for each $\mathbf{e}<q^{2m-1}$,

$$\begin{aligned}\nu^{3m-1}(I_0,\mathbf{e},0)&=\mathrm{e}\Big(\sum_{\ell=0}^{k-1}\alpha_\ell b_{3m-1}(q^{m-1}\mathbf{e}+I_{0|\ell})\Big)\\&=\mathrm{e}\Big(\alpha_{n_0}\big(b_{3m-1}(q^{m-1}\mathbf{e}+q^{m-1}-1)-b_{3m-1}(q^{m-1}\mathbf{e}+q^{m-1})\big)\Big)\\&=\mathrm{e}\Big(\alpha_{n_0}\big(b(q^{m-1}\mathbf{e}+q^{m-1}-1)-b(q^{m-1}(\mathbf{e}+1))\big)\Big).\end{aligned}$$

We find by Corollary 2.8 that there exist $\mathbf{e}_1,\mathbf{e}_2<q^{2m-1}$ such that

$$\begin{aligned}&b(q^{m-1}(\mathbf{e}_1+1)-1)-b(q^{m-1}(\mathbf{e}_1+1))\\&\qquad-b(q^{m-1}(\mathbf{e}_2+1)-1)+b(q^{m-1}(\mathbf{e}_2+1))=d\end{aligned}$$

and $\alpha_{n_0}d\notin\mathbb{Z}$.

We now compare the following two paths from $(\mathbf{0},\mathbf{0})$ to $(\mathbf{0},\mathbf{0})$ of length $m_1=n_1+n_2=\lfloor\log_q(k)\rfloor+4m-1$.

- $(\mathbf{e}_1q^{n_1}+q^{n_1}-n_0-1,\mathbf{e}_2q^{n_1}+q^{n_1}-n_0-1,1)$: we split up this path into the path of length n_1 from $(\mathbf{0},\mathbf{0})$ to (I_0,I_0) and the path of length n_2 from (I_0,I_0) to $(\mathbf{0},\mathbf{0})$. The first path can be described by the triple $(q^{n_1}-n_0-1,q^{n_1}-n_0-1,1)$, and its weight is obviously 1. The second path, *i.e.*, the path from (I_0,I_0) to $(\mathbf{0},\mathbf{0})$, can be described by the triple $(\mathbf{e}_1, \mathbf{e}_2, 0)$ and its weight equals

$$\begin{aligned}
&\nu^{n_2}(I_0, \mathbf{e}_1, 0)\overline{\nu^{n_2}(I_0, \mathbf{e}_2, 0)}\,\mathrm{e}\Big(-\frac{(\mathbf{e}_1-\mathbf{e}_2)h}{q^{\lambda-n_1}}\Big)\\
&\quad= \mathrm{e}\Big(\alpha_{n_0}(b(q^{m-1}(\mathbf{e}_1+1)-1) - b(q^{m-1}(\mathbf{e}_1+1)))\Big)\\
&\qquad\overline{\mathrm{e}(\alpha_{n_0}(b(q^{m-1}(\mathbf{e}_2+1)-1) - b(q^{m-1}(\mathbf{e}_2+1))))}\,\mathrm{e}\Big(-\frac{(\mathbf{e}_1-\mathbf{e}_2)h}{q^{\lambda-n_1}}\Big)\\
&\quad= \mathrm{e}(\alpha_{n_0}d)\,\mathrm{e}\Big(-\frac{(\mathbf{e}_1-\mathbf{e}_2)h}{q^{\lambda-n_1}}\Big).
\end{aligned}$$

Thus, the overall weight of the path from $(\mathbf{0},\mathbf{0})$ to $(\mathbf{0},\mathbf{0})$ equals

$$\mathrm{e}(\alpha_{n_0}d)\,\mathrm{e}\Big(-\frac{(\mathbf{e}_1-\mathbf{e}_2)h}{q^{\lambda-n_1}}\Big).$$

- $(\mathbf{e}_1 q^{n_1}, \mathbf{e}_2 q^{n_1}, 0)$: we compute directly the weight of this path.

$$\begin{aligned}
&\nu^{m_1}(\mathbf{0}, \mathbf{e}_1 q^{n_1}, 0)\overline{\nu^{m_1}(\mathbf{0}, \mathbf{e}_2 q^{n_1}, 0)}\,\mathrm{e}\Big(-\frac{(\mathbf{e}_1-\mathbf{e}_2)h}{q^{\lambda-n_1}}\Big)\\
&\quad= \mathrm{e}\Big(\sum_{\ell=0}^{k-1}\alpha_\ell b_{m_1}(\mathbf{e}_1 q^{n_1}) - \sum_{\ell=0}^{k-1}\alpha_\ell b_{m_1}(\mathbf{e}_2 q^{n_1})\Big)\,\mathrm{e}\Big(-\frac{(\mathbf{e}_1-\mathbf{e}_2)h}{q^{\lambda-n_1}}\Big)\\
&\quad= \mathrm{e}\Big(K(b_{m_1}(\mathbf{e}_1 q^{n_1}) - b_{m_1}(\mathbf{e}_2 q^{n_1}))\Big)\,\mathrm{e}\Big(-\frac{(\mathbf{e}_1-\mathbf{e}_2)h}{q^{\lambda-n_1}}\Big)\\
&\quad= \mathrm{e}\Big(-\frac{(\mathbf{e}_1-\mathbf{e}_2)h}{q^{\lambda-n_1}}\Big).
\end{aligned}$$

We recall briefly that $\alpha_\ell \in \{\frac{0}{m'}, \dots, \frac{m'-1}{m'}\}$ for all $\ell \in \{0, \dots, k-1\}$ and, therefore, also $\alpha_{n_0} \in \{\frac{0}{m'}, \dots, \frac{m'-1}{m'}\}$. We finally see that

$$\begin{aligned}
|B_{(\mathbf{0},\mathbf{0}),(\mathbf{0},\mathbf{0})}| &\le \Big(k_0 - 2 + \Big|\mathrm{e}(\alpha_{n_0}d)\,\mathrm{e}\Big(-\frac{(\mathbf{e}_1-\mathbf{e}_2)h}{q^{\lambda-n_1}}\Big) + \mathrm{e}\Big(-\frac{(\mathbf{e}_1-\mathbf{e}_2)h}{q^{\lambda-n_1}}\Big)\Big|\Big)q^{-3m_1}\\
&= (k_0 - 2 + |1 + \mathrm{e}(\alpha_{n_0}d)|)q^{-3m_1}\\
&= (k_0 - 2 + 2|\cos(\pi\alpha_{n_0}d)|)q^{-3m_1}\\
&= \Bigg(k_0 - 2 + 2\Big|1 - 2\Big(\sin\Big(\frac{\pi\alpha_{n_0}d}{2}\Big)\Big)^2\Big|\Bigg)q^{-3m_1}\\
&\le \Big(k_0 - 4\Big(\sin\Big(\frac{\pi}{2m'}\Big)\Big)^2\Big)q^{-3m_1}.
\end{aligned}$$

Thus we have

$$\begin{aligned}
\sum_{(J,J')}|B_{(0,0),(J,J')}| &\le \Big(k_0 - 4\Big(\sin\Big(\frac{\pi}{2m'}\Big)\Big)^2\Big)q^{-3m_1} + (1 - k_0 q^{-3m_1})\\
&\le 1 - 4\Big(\sin\Big(\frac{\pi}{2m'}\Big)\Big)^2 \cdot q^{-3m_1}.
\end{aligned}$$

Therefore, condition (3.2) of Lemma 3.1 is verified, with $m_1 = \lfloor \log_q(k)\rfloor + 4m - 1$ and $\eta = 4\big(\sin\big(\frac{\pi}{2m'}\big)\big)^2 q^{-3m_1} \ge 4\big(\sin\big(\frac{\pi}{2m'}\big)\big)^2 k^{-3} q^{-12m+3} > 0.$ ∎

To conclude this section, we want to recall the important steps of the proof of Proposition 3.7. At first we observe 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 3.7 is equivalent to $\Phi_{\lambda,\lambda'}^{I,I}(h) \ll q^{-\eta\lambda}$. Next we considered the vector $\Psi_{\lambda,\lambda'}(h) = (\Phi_{\lambda,\lambda'}^{I,I'}(h))_{(I,I')\in\mathcal{I}_k^2}$ and found the recursion

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

Then we defined $\mathbf{M}_\ell := \mathbf{M}(h/q^\ell)$ and showed that we can apply Lemma 3.1. Therefore we know that, since $|\Phi_{\lambda-\lambda'+1,0}^{I,I'}(h)| \le 1$,

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

with C and δ obtained by Lemma 3.1. Thus we know that $\Phi_{\lambda,\lambda'}^{I,I'}(h) \ll q^{-\eta\lambda}$ with $\eta = \delta/2$ uniformly for all h. This concludes the proof of Proposition 3.7.

3.4 Proof of Proposition 3.8

We again start by reducing the problem from $H_{\lambda'}^{I'}(h,d)$ to $G_\lambda^I(h,d)$ for possibly different values of λ, λ' and I, I'.

Proposition 3.15 *For $K \not\equiv 0 \pmod 1$ there exists $\eta > 0$ such that for any $I \in \mathcal{I}_k$*

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

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

Lemma 3.16 *Proposition* 3.15 *implies Proposition* 3.8.

Proof This follows directly by (3.3). ∎

Henceforth, we assume that $K \notin \mathbb{Z}$ holds. We formulate Lemma 3.6 as a matrix vector multiplication.

$$G_\lambda(h, q^j d + \delta) = \frac{1}{q^j} M_\delta^j\Big(\mathrm{e}\Big(-\frac{h}{q^\lambda}\Big)\Big) G_{\lambda-j}(h,d),$$

where for any $\delta \in \{0,\ldots,q^j - 1\}$ and $z \in \mathbb{U}$ we have

$$M_\delta^j(z) = \sum_{\varepsilon=0}^{q^j-1} \big(\mathbf{1}_{[J=T_{\varepsilon,\delta}^j(I)]}\nu^j(I,\varepsilon,\delta)z^\varepsilon\big)_{(I,J)\in\mathcal{I}_k^2}.$$

Proposition 3.15 is a consequence of the following claim:

Claim 3.17 *There exist $m_1 \in \mathbb{N}, \eta' \in \mathbb{R}^+$ such that $\|M_\delta^{m_1}(z)\|_\infty \le q^{m_1} - \eta'$ for all $\delta < q^{m_1}, z \in \mathbb{U}$.*

Lemma 3.18 *Claim* 3.17 *implies Proposition* 3.15.

https://doi.org/10.4153/CJM-2017-053-1 Published online by Cambridge University Press

Proof We first note that $\|M_\delta^j(z)\|_\infty \le q^j$ holds for all $z \in \mathbb{U}$, $j \in \mathbb{N}$, and $\delta < q^j$ by definition. Next we split the digital expansion of d mod q^L (read from left to right) into $\lfloor L/m_1 \rfloor$ parts of length m_1 and possibly one part of length L mod m_1. We denote the first parts by $\delta_1, \dots, \delta_{\lfloor L/m_1 \rfloor}$ and the last part by δ_0, *i.e.*,

$$d = q^{L \bmod m_1} \Big(\sum_{j=1}^{\lfloor L/m_1 \rfloor} \delta_j \cdot q^{\lfloor L/m_1 \rfloor - j} \Big) + \delta_0.$$

Thus we find

$$\begin{aligned}
\max_{I \in \mathfrak{I}_k} |G_\lambda^I(h,d)| &= \|G_\lambda(h,d)\|_\infty \\
&\le \frac{1}{q^L} \max_{z \in \mathbb{U}} \|M_d^L(z)\|_\infty \cdot \|G_{\lambda-L}(h, \lfloor d/q^L \rfloor)\|_\infty \\
&\le \frac{1}{q^L} \prod_{j=1}^{\lfloor L/m_1 \rfloor} \max_{z \in \mathbb{U}} \|M_{\delta_j}^{m_1}(zq^{m_1(j-1)})\|_\infty \cdot q^{(L \bmod m_1)} \cdot \|G_{\lambda-L}(h, \lfloor d/q^L \rfloor)\|_\infty \\
&\le \frac{1}{q^L} (q^{m_1} - \eta')^{\lfloor L/m_1 \rfloor} q^{(L \bmod m_1)} \cdot \|G_{\lambda-L}(h, \lfloor d/q^L \rfloor)\|_\infty \\
&\ll q^{-L\eta} \cdot \|G_{\lambda-L}(h, \lfloor d/q^L \rfloor)\|_\infty,
\end{aligned}$$

where $\eta = \frac{\eta'}{q^{m_1} \log(q^{m_1})} > 0$. ∎

The rest of this section is devoted to proving Claim 3.17. Observe that

$$\|M_\delta^{m_1'}(z)\|_\infty = \max_{I \in \mathfrak{I}_k} \max_{z \in \mathbb{U}} \sum_{J \in \mathfrak{I}_k} \Big| \sum_{\varepsilon < q^{m_1'}} \mathbf{1}_{[T_{\varepsilon,\delta}^{m_1'}(I) = J]} z^\varepsilon v^{m_1'}(I, \varepsilon, \delta) \Big|.$$

Assume that we can find, for each $I \in \mathfrak{I}_k$ and $\delta < q^{m_1}$, a pair $(\varepsilon_1, \varepsilon_2)$ and $m_1' \le m_1$ such that for all $z \in \mathbb{U}$ we have

$$\begin{aligned}
&T_{\varepsilon_i,\delta}^{m_1'}(I) = T_{\varepsilon_i+1,\delta}^{m_1'}(I) \quad \text{and} \\
&|v^{m_1'}(I, \varepsilon_1, \delta) + z v^{m_1'}(I, \varepsilon_1 + 1, \delta)| + |v^{m_1'}(I, \varepsilon_2, \delta) + z v^{m_1'}(I, \varepsilon_2 + 1, \delta)| \le 4 - \eta'.
\end{aligned} \tag{3.4}$$

This gives

$$\begin{aligned}
\max_{z \in \mathbb{U}} \sum_{J \in \mathfrak{I}_k} \Big| \sum_{\varepsilon < q^{m_1'}} \mathbf{1}_{[T_{\varepsilon,\delta}^{m_1'}(I) = J]} z^\varepsilon v^{m_1'}(I, \varepsilon, \delta) \Big| \\
&\le (q^{m_1'} - 4) + \sum_{i=1}^{2} \Big| \sum_{j=0}^{1} z^{\varepsilon_i + j} v^{m_1'}(I, \varepsilon_i + j, \delta) \Big| \\
&\le q^{m_1'} - \eta'.
\end{aligned}$$

We conclude that in total $\|M_\delta^{m_1}(z)\|_\infty \le q^{m_1 - m_1'}(q^{m_1'} - \eta') \le q^{m_1} - \eta'$, which establishes Claim 3.17.

So it remains to find $\varepsilon_1, \varepsilon_2, m_1'$ satisfying (3.4), and this turns out to be a rather tricky task.

https://doi.org/10.4153/CJM-2017-053-1 Published online by Cambridge University Press

We now fix some arbitrary $I \in \mathcal{I}_k$ and $d \in \mathbb{N}$. We start by defining, for $0 \le x \le (4m-2)k$ and $c \in \mathbb{N}$,

$$M_{x,c} = M_{x,(c \bmod q^x)} := \left\{ \ell < k : \lfloor i_\ell / q^{m-1} \rfloor + d\ell \equiv c \pmod{q^x} \right\}$$

and show some basic properties of $M_{x,c}$.

Lemma 3.19 *For every $x < q^{(4m-2)k}$ there exists c_0 such that $\sum_{\ell \in M_{x,c_0}} \alpha_\ell \notin \mathbb{Z}$.*

Proof One finds easily that $\{0, \dots, k-1\} = \bigcup_{c<q^x} M_{x,c}$, which means that

$$\{M_{x,c} : c < q^x\}$$

is a partition of $\{0, \dots, k-1\}$ for each x. Thus, we find, for every x,

$$\sum_c \sum_{\ell \in M_{x,c}} \alpha_\ell = \sum_{\ell<k} \alpha_\ell = K \notin \mathbb{Z},$$

and the proof follows easily. ∎

Lemma 3.20 *Let $d < q^{(4m-2)k}$ and $I \in \mathcal{I}_k$. Then there exists $0 \le x_0 \le (4m-2)(k-1)$ such that for each $c < q^{x_0}$ there exists $c^+ < q^{x_0+(4m-2)}$ such that $M_{x_0,c} = M_{x_0+(4m-2),c^+}$.*

Remark 3.21 This is equivalent to the statement that

$$\lfloor i_{\ell_1} / q^{m-1} \rfloor + d\ell_1 \equiv \lfloor i_{\ell_2} / q^{m-1} \rfloor + d\ell_2 \pmod{q^{x_0}}$$

implies

$$\lfloor i_{\ell_1} / q^{m-1} \rfloor + d\ell_1 \equiv \lfloor i_{\ell_2} / q^{m-1} \rfloor + d\ell_2 \pmod{q^{x_0+4m-2}}$$

Proof We have already seen that $\{M_{x,c} : c < q^x\}$ is a partition of $\{0, \dots, k-1\}$. Furthermore, we find for $0 \le x \le (4m-2)k$ and $c < q^x$ that

$$M_{x,c} = \bigcup_{c' < q^{4m-2}} M_{x+(4m-2),c+q^x c'}.$$

This implies that $\{M_{x+4m-2,c} : c < q^{x+4m-2}\}$ is a refinement of $\{M_{x,c} : c < q^x\}$ and we find

$$\begin{aligned}\{M_{(4m-2)\cdot 0,c} : c < 1\} &\ge \{M_{(4m-2)\cdot 1,c} : c < q^{4m-2}\} \\ &\ge \cdots \ge \{M_{(4m-2)k,c} : c < q^{(4m-2)k}\}.\end{aligned}$$

It is well known that k is the maximal length of a chain in the set of partitions of $\{0, \dots, k-1\}$. This means that there exists x_0' such that

$$\{M_{(4m-2)x_0',c} : c < q^{(4m-2)x_0'}\} = \{M_{(4m-2)(x_0'+1),c'} : c' < q^{(4m-2)(x_0'+1)}\}. \qquad ∎$$

Next, we define $\beta_{x,c} := \sum_{\ell \in M_{x,c}} \alpha_\ell$.

We can now choose $m_1 := (4m-2)k$, $m_1' := x_0 + (4m-2)$, where x_0 is given by Lemma 3.20. We consider $c_0 < q^{x_0}$ and c_0^+ provided by Lemmas 3.19 and 3.20, and we know that $\beta_{x_0,c_0} \notin \mathbb{Z}$. Therefore we apply Corollary 2.8 and find $\mathbf{e}_1, \mathbf{e}_2 < q^{2m-1}$ such that

$$b(q^{m-1}(\mathbf{e}_1+1)-1) - b(q^{m-1}(\mathbf{e}_1+1)) - b(q^{m-1}(\mathbf{e}_2+1)-1) + b(q^{m-1}(\mathbf{e}_2+1)) = d,$$

and $d\beta_{x_0,c_0} \notin \mathbb{Z}$.

https://doi.org/10.4153/CJM-2017-053-1 Published online by Cambridge University Press

We are now able to define

$$\varepsilon_1 = \left(q^{x_0+m-1}(\mathbf{e}_1+1) - c_0^+ - 1\right) \bmod q^{x_0+4m-2}$$
$$\varepsilon_2 = \left(q^{x_0+m-1}(\mathbf{e}_2+1) - c_0^+ - 1\right) \bmod q^{x_0+4m-2}.$$

It only remains to check (3.4), which we split up into the following two lemmata.

Lemma 3.22 *Let x_0, ε_i be defined as above. Then $T^{x_0+4m-2}_{\varepsilon_i,d}(I) = T^{x_0+4m-2}_{\varepsilon_i+1,d}(I)$.*

Proof We need to show that

$$\left\lfloor \frac{i_\ell + q^{m-1}(\ell d + \varepsilon_i)}{q^{x_0+4m-2}} \right\rfloor = \left\lfloor \frac{i_\ell + q^{m-1}(\ell d + \varepsilon_i + 1)}{q^{x_0+4m-2}} \right\rfloor \tag{3.5}$$

holds for all $\ell < k$ and $i = 1, 2$. We know that ℓ belongs to M_{x_0+4m-2,c^+} for some $c < q^{x_0}$. Thus, we find for $j = 0, 1$

$$\left\lfloor \frac{i_\ell + q^{m-1}(\ell d + \varepsilon_i + j)}{q^{x_0+4m-2}} \right\rfloor = \left\lfloor \frac{(i_\ell \bmod q^{m-1}) + q^{m-1}(c^+ + \varepsilon_i + j)}{q^{x_0+4m-2}} \right\rfloor$$
$$= \left\lfloor \frac{c^+ + \varepsilon_i + j}{q^{x_0+3m-1}} \right\rfloor.$$

Therefore, (3.5) does hold, unless $c^+ + \varepsilon_i + 1 \equiv 0 \pmod{q^{x_0+3m-1}}$. We find that

$$c^+ + \varepsilon_i + 1 \equiv c^+ + q^{x_0+m-1}(\mathbf{e}_i + 1) - c_0^+ \pmod{q^{x_0+3m-1}}.$$

We first consider the case $c \not\equiv c_0$: $c^+ + \varepsilon_i + 1 \equiv c - c_0 \not\equiv 0 \pmod{q^{x_0}}$. For $c = c_0$,

$$c_0^+ + \varepsilon_i + 1 \equiv q^{x_0+m-1}(\mathbf{e}_i + 1) \pmod{q^{x_0+3m-1}}.$$

However $\mathbf{e}_i + 1 \not\equiv 0 \pmod{q^{2m}}$ as $\mathbf{e}_i < q^{2m-1}$. Thus, (3.5) holds. ∎

Lemma 3.23 *There exists $\eta' > 0$, depending only on m', such that for x_0 and ε_i, defined as above,*

$$\sum_{i=1}^{2} \left| \nu^{x_0+4m-2}(I, \varepsilon_i, \delta) + z \cdot \nu^{x_0+4m-2}(I, \varepsilon_i + 1, \delta) \right| \le 4 - \eta' \tag{3.6}$$

holds for all $z \in \mathbb{U}$.

Proof We start by computing the weights $\nu^{x_0+4m-2}(I, \varepsilon_i + j, \delta)$. For arbitrary $\varepsilon < q^{\lambda_0+4m-2}$, we find

$$\begin{aligned}
&\nu^{x_0+4m-2}(I, \varepsilon, d)\\
&\quad = \prod_{\ell<k} \mathrm{e}\left(\alpha_\ell b_{x_0+4m-2}(i_\ell + q^{m-1}(\varepsilon + \ell d)) \right)\\
&\quad = \prod_{\ell<k} \mathrm{e}\left(\alpha_\ell b_{m-1}(i_\ell + q^{m-1}(\varepsilon + \ell d)) \right) \mathrm{e}\left(\alpha_\ell b_{x_0+3m-1}(\lfloor i_\ell / q^{m-1} \rfloor + \varepsilon + \ell d) \right)\\
&\quad = \mathrm{e}(g(\varepsilon)) \prod_{\ell<k} \mathrm{e}(\alpha_\ell b_{x_0+3m-1}(\lfloor i_\ell / q^{m-1} \rfloor + \varepsilon + \ell d)),
\end{aligned}$$

where $g(\varepsilon) := \sum_{\ell<k} \alpha_\ell b_{m-1}(i_\ell + q^{m-1}(\varepsilon + \ell d))$. Note that $g(\varepsilon)$ only depends on $\varepsilon \bmod q^{m-1}$.

We can describe this product by using the weights β defined above.

$$\nu^{x_0+4m-2}(I,\varepsilon,d) = \mathrm{e}(g(\varepsilon)) \prod_{c'<q^{x_0+4m-2}} \mathrm{e}(\beta_{x_0+4m-2,c'} b_{x_0+3m-1}(c'+\varepsilon)).$$

Furthermore, we can rewrite every $c' < q^{x_0+4m-2}$ for which $\beta_{x_0+4m-2,c'} \neq 0$ as some c^+ where $c < q^{x_0}$. This gives then

$$\begin{aligned}\nu^{x_0+4m-2}(I,\varepsilon,d) &= \mathrm{e}(g(\varepsilon)) \cdot \prod_{c<q^{x_0}} \mathrm{e}(\beta_{x_0,c} \cdot b_{x_0+3m-1}(c^+ + \varepsilon))\\ &= \mathrm{e}(g(\varepsilon)) \cdot \prod_{c<q^{x_0}} \mathrm{e}(\beta_{x_0,c} \cdot b_{x_0}(c^+ + \varepsilon)) \cdot \prod_{c<q^{x_0}} \mathrm{e}\Big(\beta_{x_0,c} \cdot b_{3m-1}\Big(\Big\lfloor \frac{c^+ + \varepsilon}{q^{x_0}} \Big\rfloor\Big)\Big)\end{aligned}$$

Thus we find for $\varepsilon = \varepsilon_i + j$ that

$$\begin{aligned}&\nu^{x_0+4m-2}(I,\varepsilon_i + j,d)\\ &\quad= \mathrm{e}(g(\varepsilon_i + j)) \cdot \prod_{c<q^{x_0}} \mathrm{e}(\beta_{x_0,c} \cdot b_{x_0}(c^+ + \varepsilon_i + j))\\ &\qquad\times \prod_{c<q^{x_0}} \mathrm{e}\Big(\beta_{x_0,c} \cdot b_{3m-1}\Big(\Big\lfloor \frac{c^+ + \varepsilon_i + j}{q^{x_0}} \Big\rfloor\Big)\Big)\\ &\quad= \mathrm{e}(g(-c_0^+ - 1 + j)) \cdot \prod_{c<q^{x_0}} \mathrm{e}(\beta_{x_0,c} \cdot b_{x_0}(c^+ - c_0^+ - 1 + j))\\ &\qquad\times \prod_{c<q^{x_0}} \mathrm{e}\Big(\beta_{x_0,c} \cdot b_{3m-1}\Big(q^{m-1}(\mathbf{e}_i + 1) + \Big\lfloor \frac{c^+ - c_0^+ - 1 + j}{q^{x_0}} \Big\rfloor\Big)\Big)\\ &\quad= \mathrm{e}(g(-c_0^+ - 1 + j)) \cdot \prod_{c<q^{x_0}} \mathrm{e}(\beta_{x_0,c} \cdot b_{x_0}(c^+ - c_0^+ - 1 + j))\\ &\qquad\times \prod_{\substack{c<q^{x_0}\\ c\neq c_0}} \mathrm{e}\Big(\beta_{x_0,c} \cdot b_{3m-1}\Big(q^{m-1}(\mathbf{e}_i + 1) + \Big\lfloor \frac{c^+ - c_0^+ - 1 + j}{q^{x_0}} \Big\rfloor\Big)\Big)\\ &\qquad\times \mathrm{e}(\beta_{x_0,c_0} \cdot b_{3m-1}(q^{m-1}(\mathbf{e}_i + 1) - 1 + j)).\end{aligned}$$

For $c \neq c_0$, we find $\lfloor \frac{c^+ - c_0^+ - 1}{q^{x_0}} \rfloor = \lfloor \frac{c^+ - c_0^+}{q^{x_0}} \rfloor$ as $c^+ \equiv c \not\equiv c_0 \equiv c_0^+ \mod q^{x_0}$.
Consequently, we find

$$\nu^{x_0+4m-2}(I,\varepsilon_i,d) = \mathrm{e}(x_i), \quad \nu^{x_0+4m-2}(I,\varepsilon_i + 1,d) = \mathrm{e}(x_i + \xi_i),$$

where

$$\begin{aligned}x_i = g(-c_0^+ - 1) &+ \sum_{c<q^{x_0}} \beta_{x_0,c} \cdot b_{x_0}(c^+ - c_0^+ - 1)\\ &+ \sum_{\substack{c<q^{x_0}\\ c\neq c_0}} \beta_{x_0,c} \cdot b_{3m-1}\Big(q^{m-1}(\mathbf{e}_i + 1) + \Big\lfloor \frac{c^+ - c_0^+}{q^{x_0}} \Big\rfloor\Big)\\ &+ \beta_{x_0,c_0} \cdot b_{3m-1}(q^{m-1}(\mathbf{e}_i + 1) - 1)\end{aligned}$$

https://doi.org/10.4153/CJM-2017-053-1 Published online by Cambridge University Press

and

$$\xi_i = g(-c_0^+) + \sum_{c<q^{x_0}} \beta_{x_0,c} \cdot b_{x_0}(c^+ - c_0^+) + \beta_{x_0,c_0} \cdot b_{3m-1}(q^{m-1}(\mathbf{e}_i + 1))$$
$$- g(-c_0^+ - 1) - \sum_{c<q^{x_0}} \beta_{x_0,c} \cdot b_{x_0}(c^+ - c_0^+ - 1) - \beta_{x_0,c_0} \cdot b_{3m-1}(q^{m-1}(\mathbf{e}_i + 1) - 1).$$

Also, we find $\xi_1 - \xi_2 = \beta_{x_0,c_0} d \notin \mathbb{Z}$, where

$$b(q^{m-1}(\mathbf{e}_1 + 1)) - b(q^{m-1}(\mathbf{e}_1 + 1) - 1) - b(q^{m-1}(\mathbf{e}_2 + 1)) + b(q^{m-1}(\mathbf{e}_2 + 1) - 1) = d.$$

This implies $\|\xi_1 - \xi_2\| \geq \frac{1}{m'}$.

It remains to apply Lemma 3.2 to find that (3.6) holds with $\eta' = 8(\sin(\frac{\pi}{4m'}))^2$. ■

To finish of this section, we recall the important steps of the proof of Proposition 3.15. We began by rewriting our recursion for G_λ^I as a matrix vector multiplication, $G_\lambda(h, q^L d + \delta) = \frac{1}{q^L} M_\delta^L(\mathrm{e}(-\frac{h}{q^\lambda}))G_{\lambda-L}(h,d)$. We then split up this matrix $M_\delta^L(\cdot)$ into a product of many matrices $M_{\delta_j}^{m_1}(\cdot)$, where $m_1 = (4m-2)k$. Then we showed that $\|M_{\delta_j}^{m_1}(\cdot)\| \leq q^{m_1} - \eta$, where $\eta = 8(\sin(\frac{\pi}{4m'}))^2$. This then implies Proposition 3.15. To show that $\|M_{\delta_j}^{m_1}\| \leq q^{m_1} - \eta$, we found two different ε_i such that

$$T_{\varepsilon_i,\delta}^{m_1'}(I) = T_{\varepsilon_i+1,\delta}^{m_1'}(I) \quad \text{and}$$
$$|v^{m_1'}(I, \varepsilon_1, \delta) + z v^{m_1'}(I, \varepsilon_1 + 1, \delta)| + |v^{m_1'}(I, \varepsilon_2, \delta) + z v^{m_1'}(I, \varepsilon_2 + 1, \delta)| \leq 4 - \eta'$$

holds for all $z \in \mathbb{U}$.

4 Proof of the Main Theorem

In this section, we complete the proof of Theorem 1.6 following the ideas and structure of [6]. As the proof is very similar, we only outline it briefly and comment on the important changes.

The structure of the proof is similar for both cases. First we want to substitute the function b by $b_{\mu,\lambda}$. This can be done by applying Lemmas 5.5 and 5.7 in the case $K \in \mathbb{Z}$. For the case $K \notin \mathbb{Z}$ we must use Lemma 5.7 first.

Thereafter, we apply Lemma 5.6 to detect the digits between μ and λ. Next, we use characteristic functions to detect suitable values for $u_1(n)$, $u_2(n)$, $u_3(n)$. Lemma 5.9 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 apply either Proposition 3.7 or Proposition 3.8, depending on whether $K \in \mathbb{Z}$.

The case $K \notin \mathbb{Z}$ needs more effort to deal with.

4.1 The Case $K \in \mathbb{Z}$

In this section, we show that if $K = \alpha_0 + \cdots + \alpha_{k-1} \in \mathbb{Z}$, Proposition 3.7 provides an upper bound for the sum

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

https://doi.org/10.4153/CJM-2017-053-1 Published online by Cambridge University Press

Let ν be the unique integer such that $q^{\nu-1} < N \leq q^{\nu}$, and we choose all appearing exponents, *i.e.*, λ, μ, ρ, as in [6].

By using Lemma 5.5 and the same arguments as in [6], we find that

$$S_0 = S_1 + \mathcal{O}(q^{\nu-(\lambda-\nu)}),$$

where

$$S_1 = \sum_{n<N} \mathrm{e}\Big(\sum_{\ell=0}^{k-1} \alpha_\ell b_\lambda((n+\ell)^2) \Big).$$

Now we use Lemma 5.7, with $Q = q^{\mu+m-1}$ and $S = q^{\nu-\mu}$, to relate S_1 to a sum in terms of $b_{\mu,\lambda}$: $|S_1|^2 \ll \frac{N^2}{S} + \frac{N}{S}\mathfrak{R}(S_2)$, where $S_2 = \sum_{1\leq s<S}\big(1-\frac{s}{S}\big) S_2'(s)$ and

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

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

Next we use Lemma 5.6 to detect the digits of $(n+\ell)^2$ and $(n+\ell+sq^{m-1}q^{\mu})^2$ between μ and $\lambda+m-1$, with a negligible error term. Therefore, we must take the digits between $\mu' = \mu - \rho'$ and μ into account, where $\rho' > 0$ will be chosen later.

We choose the integers $u_1 = u_1(n)$, $u_3 = u_3(n)$, $\nu = \nu(n)$, $w_1 = w_1(n)$, and $w_3 = w_3(n)$ to satisfy the conditions of Lemma 5.6 and detect them by characteristic functions. Thus, we find $S_2'(s) = S_3'(s) + \mathcal{O}(q^{\nu-\rho'})$, where

$$\begin{aligned} S_3'(s) = \sum_{0\leq u_1<U_1} \sum_{0\leq u_3<U_3} \sum_{n\in I(N,s)} \Bigg(&\chi_{q^{\mu'-\lambda-m+1}}\Big(\frac{n^2}{q^{\lambda+m-1}} - \frac{u_1}{U_1}\Big) \chi_{q^{\mu'-\nu-1}}\Big(\frac{2n}{q^{\nu+1}} - \frac{u_3}{U_3}\Big) \\ \times \mathrm{e}\Big(\sum_{\ell=0}^{k-1} \alpha_\ell \big(&b_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3) - b_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+\nu(n)q^{\rho'} + 2\ell s q^{m-1}q^{\rho'}) \big) \Big) \Bigg), \end{aligned}$$

where χ_α is defined by (5.2) and $U_1 = q^{\lambda+m-1-\mu'}$, $U_3 = q^{\nu-\mu'+1}$. Lemma 5.9 allows us to replace the characteristic functions χ by trigonometric polynomials. More precisely, using (5.4) with $H_1 = U_1 q^{\rho''}$ and $H_3 = U_3 q^{\rho''}$ for some suitable $\rho'' > 0$ (which is a fraction of ν chosen later), we have $S_3'(s) = S_4(s) + \mathcal{O}(E_1) + \mathcal{O}(E_3) + \mathcal{O}(E_{1,3})$, where E_1, E_3, and $E_{1,3}$ are the error terms specified in (5.4) and

$$\begin{aligned} S_4(s) = &\sum_{0\leq u_1<U_1} \sum_{0\leq u_3<U_3} \sum_{0\leq \nu<q^{\lambda-\mu+m-1}} \sum_{n\in I(N,s)} \\ &\Bigg(A_{U_1^{-1},H_1}\Big(\frac{n^2}{q^{\lambda+m-1}} - \frac{u_1}{U_1}\Big) A_{U_3^{-1},H_3}\Big(\frac{2n}{q^{\nu+1}} - \frac{u_3}{U_3}\Big) \\ &\quad \times \mathrm{e}\Big(\sum_{\ell=0}^{k-1} \alpha_\ell \big(b_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3) - b_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+\nu q^{\rho'} + 2\ell s q^{m-1}q^{\rho'}) \big) \Big) \\ &\quad \times \frac{1}{q^{\lambda-\mu+m-1}} \sum_{0\leq h<q^{\lambda-\mu+m-1}} \mathrm{e}\Big(h \frac{2sq^{m-1}n - \nu}{q^{\lambda-\mu+m-1}} \Big) \Bigg), \end{aligned}$$

where we use the last sum to detect the correct value of $\nu = \nu(n)$.

The error terms E_1, E_3, $E_{1,3}$ can easily be estimated with the help of Lemma 5.4, just as in [6].

By using the representations of $A_{U_1^{-1},H_1}$ and $A_{U_3^{-1},H_3}$, we obtain

$$S_4(s) = \frac{1}{q^{\lambda-\mu+m-1}} \sum_{|h_1|\le H_1} \sum_{|h_3|\le H_3} \sum_{0\le h<q^{\lambda-\mu+m-1}} a_{h_1}(U_1^{-1},H_1)\, a_{h_3}(U_3^{-1},H_3)$$
$$\sum_{0\le u_1<U_1} \sum_{0\le u_3<U_3} \sum_{0\le v<q^{\lambda-\mu+m-1}} \mathrm{e}\Big(-\frac{h_1u_1}{U_1} - \frac{h_3u_3}{U_3} - \frac{hv}{q^{\lambda-\mu+m-1}}\Big)$$
$$\mathrm{e}\Big(\sum_{\ell=0}^{k-1} \alpha_\ell\big(b_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3) - b_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3 + vq^{\rho'} + 2\ell s q^{m-1}q^{\rho'})\big)\Big)$$
$$\cdot \sum_n \mathrm{e}\Big(\frac{h_1n^2}{q^{\lambda+m-1}} + \frac{h_3n}{q^v} + \frac{2hsn}{q^{\lambda-\mu}}\Big).$$

We now distinguish the cases $h_1 = 0$ and $h_1 \ne 0$. For $h_1 \ne 0$, we can estimate the exponential sum by using Lemma 5.4 and the estimate

$$\sum_{1\le h_1\le H_1} \sqrt{\gcd(h_1,q^\lambda)} \ll_q H_1.$$

Thus, we find

$$\sum_{0<|h_1|\le H_1} \sum_{|h_3|\le H_3} \sum_{h=0}^{q^{\lambda-\mu+m-1}-1} \Big|\sum_n \mathrm{e}\Big(\frac{h_1n^2}{q^{\lambda+m-1}} + \frac{h_3n}{q^v} + \frac{2hsn}{q^{\lambda-\mu}}\Big)\Big| \ll \lambda H_1H_3 q^{\lambda/2+\lambda-\mu}.$$

This then gives $S_4(s) = S_5(s) + \mathcal{O}(\lambda q^{3\lambda/4})$, where $S_5(s)$ denotes the part of $S_4(s)$ with $h_1 = 0$.

We set $u_1 = u_1'' + q^{\rho'}u_1'$ and $u_3 = u_3'' + q^{\rho'}u_3'$, where $0 \le u_1'', u_3'' < q^{\rho'}$. Furthermore, we define $i_\ell = \lfloor (u_1'' + \ell u_3'')/q^{\rho'}\rfloor$. 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, by the same arguments as in [6],

$$S_5(s) \le \sum_{|h_3|\le H_3} \sum_{0\le h<q^{\lambda-\mu+m-1}} \frac{1}{q^{v+1-\mu}}$$
$$\times \sum_{0\le u_3'<q^{v-\mu+1}} \sum_{I\in\mathcal{I}_k} \big|H^I_{\lambda-\mu}(h,u_3')\overline{H^I_{\lambda-\mu}(h,u_3'+2sq^{m-1})}\big|$$
$$\times \min\Big(N, \Big|\sin\Big(\pi\Big(\frac{h_3}{q^v} + \frac{2hs}{q^{\lambda-\mu}}\Big)\Big)\Big|^{-1}\Big).$$

Using the estimate $|H^I_{\lambda-\mu}(h,u_3'+2sq^{m-1})| \le 1$ and the Cauchy–Schwarz inequality yields

$$\sum_{0\le u_3'<q^{v-\mu+1}} \big|H^I_{\lambda-\mu}(h,u_3')\overline{H^I_{\lambda-\mu}(h,u_3'+2sq^{m-1})}\big|$$
$$\le q^{(v-\mu+1)/2}\Big(\sum_{0\le u_3'<q^{v-\mu+1}} \big|H^I_{\lambda-\mu}(h,u_3')\big|^2\Big)^{1/2}.$$

We now replace λ by $\lambda-\mu+m-1$, λ' by $v-\mu+1$ and apply Proposition 3.7:

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

https://doi.org/10.4153/CJM-2017-053-1 Published online by Cambridge University Press

Next we average over s and h, as in [6], by applying Lemma 5.2. Thus we have a factor $\tau(q^{\lambda-\mu}) \ll_q (\lambda-\mu)^{\omega(q)}$ compared to $\tau(2^{\lambda-\mu}) = \lambda-\mu+1$. Combining all the estimates as in [6] then gives

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

provided that the following conditions hold:

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

For example, the choice $\lambda = \nu + \lfloor \frac{\nu}{20} \rfloor$ and $\rho' = \rho'' = \lfloor \frac{\nu}{200} \rfloor$ ensures that the above conditions are satisfied.

Summing up we proved that for $\eta' < \min(1/200, \eta/40)$, where η is given by Proposition 3.7, $S_0 \ll q^{\nu(1-\eta')} \ll N^{1-\eta'}$ holds, which is precisely the statement of Theorem 1.6.

4.2 The Case $K \notin \mathbb{Z}$

In this section we show that, for $K = \alpha_0 + \cdots + \alpha_{k-1} \notin \mathbb{Z}$, Proposition 3.8 provides an upper bound for the sum $S_0 = \sum_{n<N} \mathrm{e}(\sum_{\ell=0}^{k-1} \alpha_\ell b((n+\ell)^2))$.

Let μ, λ, ρ, and ρ_1 be integers satisfying

$$0 \le \rho_1 < \rho < \mu = \nu - 2\rho < \nu < \lambda = \nu + 2\rho < 2\nu, \tag{4.1}$$

to be chosen later, just as in [6]. Since $K \notin \mathbb{Z}$ we cannot use Lemma 5.5 directly. Therefore, we apply Lemma 5.7 with $Q = 1$ and $R = q^{\rho}$. Summing trivially for $1 \le r \le R_1 = q^{\rho_1}$ yields $|S_0|^2 \ll \frac{N^2 R_1}{R} + \frac{N}{R} \sum_{R_1<r<R} \big(1-\frac{r}{R}\big) \Re(S_1(r))$, where

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

and $I_1(r)$ is an interval included in $[0, N-1]$. By Lemma 5.5 we conclude that

$$b_{\lambda,\infty}((n+\ell)^2) = b_{\lambda,\infty}((n+r+\ell)^2)$$

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 $S_1'(r) = \sum_{n\in I_1(r)} \mathrm{e}\big(\sum_{\ell=0}^{k-1} \alpha_\ell (b_\lambda((n+\ell)^2) - b_\lambda((n+r+\ell)^2))\big)$. This leads to

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

and the Cauchy–Schwarz inequality gives

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

For $|S_1'(r)|^2$ we can use Lemma 5.7 again: let $\rho' \in \mathbb{N}$, to be chosen later, be such that $1 \le \rho' \le \rho$. After applying Lemma 5.7 with $Q = q^{\mu+m-1}$ and

$$S = q^{2\rho'} \le q^{\nu-\mu}, \tag{4.2}$$

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

$$b_\lambda((\widetilde{n} + sq^{\mu+m-1})^2) - b_\lambda(\widetilde{n}^2) = b_{\mu,\lambda}((\widetilde{n} + sq^{\mu+m-1})^2) - b_{\mu,\lambda}(\widetilde{n}^2),$$

and thus

$$|S_0|^4 \ll q^{4\nu-2\rho+2\rho_1} + q^{6\nu+2\rho-2\lambda} + \frac{q^{4\nu}}{S} + \frac{q^{3\nu}}{RS} \sum_{R_1<r<R} \sum_{1\le s<S} |S_2(r,s)|, \tag{4.3}$$

with

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

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

We now apply a Fourier analysis similar to the case $K \equiv 0 \pmod 1$ [6]. We set $U = q^{\lambda+m-1-\mu'}$, $U_3 = q^{\nu-\mu'+1}$, and $V = q^{\lambda-\mu+m-1}$. We apply Lemma 5.6 and detect the correct values of u_1, u_2, u_3 by characteristic functions. This gives

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

Furthermore, we use Lemma 5.9 to replace the characteristic functions χ by trigonometric polynomials. Using (5.4) with $U_1 = U_2 = U$, $H_1 = H_2 = Uq^{\rho_2}$, and $H_3 = U_3 q^{\rho_3}$, and integers ρ_2, ρ_3 satisfying $\rho_2 \le \mu - \rho'$, $\rho_3 \le \mu - \rho'$, we obtain

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

for the error terms obtained by (5.4) and $S_3(r,s)$ obtained by replacing the characteristic function by trigonometric polynomials. We now reformulate $S_3(r,s)$ by expanding the trigonometric polynomials, detecting the correct value of $\nu = \nu(n)$, and restructuring the sums:

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

One can estimate the error terms just as in [6] and find that they are bounded by either $q^{\nu-\rho_3}$ or $q^{\nu-\rho_2}$. In conclusion, we deduce that

$$S_2(r,s) = S_3(r,s) + \mathcal{O}(q^{\nu-\rho'}) + \mathcal{O}(q^{\nu-\rho_2}) + \mathcal{O}(q^{\nu-\rho_3}). \tag{4.4}$$

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

$$S_3(r,s) = S_4(r,s) + S_4'(r,s), \tag{4.5}$$

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 $h_1+h_2\ne 0$. We can estimate $S_4'(r,s)$ as in [6] and find $S_4'(r,s) \ll \nu^4 q^{\nu+\frac12(8\lambda-9\mu+7\rho'+\rho_2)}$, and 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 block-additive function by a truncated block-additive function:

$$b_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3) = b_{\lambda-\mu}\big(u_1'+\ell u_3' + \lfloor (u_1''+\ell u_3'')/q^{\rho'}\rfloor\big),$$
$$b_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3) = b_{\lambda-\mu}\big(u_2'+\ell u_3' + \lfloor (u_2''+\ell u_3'')/q^{\rho'}\rfloor\big),$$
$$b_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+vq^{\rho'}+2\ell sq^{m-1}q^{\rho'}) =$$
$$b_{\lambda-\mu}\big(u_1'+v+\ell(u_3'+2sq^{m-1}) + \lfloor (u_1''+\ell u_3'')/q^{\rho'}\rfloor\big),$$
$$b_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3+vq^{\rho'}+2(\ell+r)sq^{m-1}q^{\rho'}) =$$
$$b_{\lambda-\mu}\big(u_2'+v+2srq^{m-1}+\ell(u_3'+2sq^{m-1}) + \lfloor (u_2''+\ell u_3'')/q^{\rho'}\rfloor\big).$$

Using the periodicity of b modulo $V := q^{\lambda-\mu+m-1}$, we replace the variable v by v_1 such that $v_1 \equiv u_1'+v \pmod{q^{\lambda-\mu+m-1}}$. Furthermore we introduce a new variable v_2 such that $v_2 \equiv u_2'+v+2srq^{m-1} \equiv v_1+u_2'-u_1'+2srq^{m-1} \pmod{q^{\lambda-\mu+m-1}}$. We then follow

https://doi.org/10.4153/CJM-2017-053-1 Published online by Cambridge University Press

the arguments of [6] and find

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

with

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

The next few steps are again very similar to the corresponding ones in [6], and we skip the details. We find

$$\begin{aligned} S_4(r,s) \ll{}& (\lambda-\mu)\ \gcd(2s, q^{\lambda-\mu})\ q^{2\lambda-2\mu} \\ &\times \sum_{0\le u_1'',u_2'',u_3''<q^{\rho'}} \sum_{|h_2|\le H_2} \min(U^{-2},h_2^{-2}) S_6(h_2,s,u_1'',u_3'')^{1/2} S_6(h_2,s,u_2'',u_3'')^{1/2} \\ &\times \sum_{|h_3|\le H_3} \min(U_3^{-1},h_3^{-1}) \min\Big(q^{\nu}, \Big| \sin\pi \frac{2h_2r + 2q^{\lambda-\nu+m-1}h_3}{q^{\lambda+m-1}} \Big|^{-1} \Big), \end{aligned}$$

where

$$\begin{aligned} S_6(h_2,s,u'',u_3'') = \sum_{0\le u_3'<U_3'} &\sum_{0\le h'<q^{\lambda-\mu+m-1}} \\ &|H_{\lambda-\mu}^{I(u'',u_3'')}(h'-h_2,u_3')|^2 |H_{\lambda-\mu}^{I(u'',u_3'')}(h',u_3'+2sq^{m-1})|^2. \end{aligned}$$

Here we introduce the integers H_2' and κ such that

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

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 $|h_2| \le H_2'$, $H_2' < |h_2| \le q^{\lambda+m-1-\mu}$, and $q^{\lambda+m-1-\mu} < |h_2| \le H_2$, respectively.

Estimate of $S_{41}(r,s)$ By (5.1) we have

$$\sum_{|h_3|\le H_3} \min\Big(q^{\nu}, \Big| \sin\pi \frac{2h_3 + 2h_2rq^{\nu-\lambda-m+1}}{q^{\nu}} \Big|^{-1} \Big) \ll \nu q^{\nu},$$

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

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

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

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

We obtain $\sum_{|h_2|\le H_2'} |H_{\lambda-\mu}^{I(u'',u_3'')}(h'-h_2,u_3')|^2 \ll q^{-\eta'(\lambda-\mu-\kappa)} = \big(\frac{H_2'}{q^{\lambda-\mu}}\big)^{\eta'}$ uniformly in λ, μ, H_2', u_3', u'', and u_3''.

The remaining proof is analogous to the corresponding proof in [6]. The only difference is again that by using Lemma 5.2 we obtain a factor $(\lambda-\mu)^{\omega(q)}$ instead of $(\lambda-\mu)$. This gives

$$\frac{1}{RS}\sum_{R_1<r<R}\sum_{1\le s<S} S_{41}(r,s) \ll \nu(\lambda-\mu)^{\omega(q)+1}\, q^{\nu-\eta'(\rho_1-\rho'-\rho_3)}, \tag{4.6}$$

which concludes this part.

Estimate of $S_{42}(r,s)$ and $S_{43}(r,s)$ By following the arguments of [6] and applying the same changes as in the estimate of S_{41} we find

$$\frac{1}{RS}\sum_{R_1<r<R}\sum_{1\le s<S} S_{42}(r,s) \ll \rho(\lambda-\mu)^{2+\omega(q)}\, q^{\nu-\rho+\rho_1+\rho'-\rho_3}, \tag{4.7}$$

$$\frac{1}{RS}\sum_{R_1<r<R}\sum_{1\le s<S} S_{43}(r,s) \ll \rho\,(\lambda-\mu)^{2+\omega(q)}\, q^{\nu-\rho+3\rho'}. \tag{4.8}$$

Combining the estimates for S_4 It follows from (4.6), (4.7), and (4.8) that

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

Choosing $\rho_1=\rho-\rho'$ and $\rho_2=\rho_3=\rho'$, we obtain

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

Since $0<\eta'<1$, we obtain using (4.5) and (4.4) that

$$\frac{1}{RS}\sum_{R_1<r<R}\sum_{1\le s<S} S_2(r,s) \ll \nu^{3+\omega(q)} q^\nu \big(q^{-\eta'(\rho-3\rho')} + q^{-\rho'} + q^{\frac12(8\lambda-9\mu+8\rho')}\big).$$

We recall from (4.2) that $S = q^{2\rho'}$ and from (4.1) that $\mu = \nu - 2\rho$, $\lambda = \nu + 2\rho$, and we insert the estimation from above in (4.3),

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

For $\rho' = \lfloor \nu/146 \rfloor$ and $\rho = 4\rho'$, we obtain $|S_0| \ll \nu^{(3+\omega(q))/4} q^{\nu - \frac{\eta'\rho'}{4}} \ll N^{1-\eta_1}$, for all $\eta_1 < \eta'/584$. Therefore we have seen that Proposition 3.8 implies the case $K \not\equiv 0 \pmod 1$ of Theorem 1.6.

5 Auxiliary Results

In this last section, we present some auxiliary results that are used in Section 4 to prove the main theorem. For this proof, it is crucial to approximate characteristic functions of the intervals $[0, \alpha) \bmod 1$ where $0 \le \alpha < 1$ by trigonometric polynomials. This is done by using Vaaler's method (see Section 5.5). As we deal with exponential sums, we also use a generalization of Van der Corput's inequality that we will see in Section 5.4. In Section 5.1, we acquire some results dealing with sums of geometric series that we use to bound linear exponential sums. Section 5.2 is dedicated to one classic result on Gauss sums and allows us to find appropriate bounds on the occurring quadratic exponential sums in Section 4. The last part of this section deals with carry propagation. We find a quantitative statement that carry propagation along several digits is rare, *i.e.*, exponentially decreasing. We would like to note that all these auxiliary results have already been presented in [6].

5.1 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 $L_1, L_2 \in \mathbb{Z}$, $L_1 \le L_2$

$$\Big| \sum_{L_1 < \ell \le L_2} \mathrm{e}(\ell\xi) \Big| \le \min(L_2 - L_1, |\sin \pi\xi|^{-1}),$$

that 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 5.1 *Let $(a, m) \in \mathbb{Z}^2$ with $m \ge 1$, $\delta = \gcd(a, m)$, and $b \in \mathbb{R}$. For any real number $U > 0$, we have*

$$\sum_{0 \le n < m} \min\Big(U, \Big| \sin\Big(\pi \frac{an+b}{m} \Big) \Big|^{-1} \Big) \le \delta \min\Big(U, \Big| \sin\Big(\pi \frac{\delta \, \|b/\delta\|}{m} \Big) \Big|^{-1} \Big) + \frac{2m}{\pi} \log(2m). \tag{5.1}$$

Proof This is [6, Lemma 6]. ∎

Lemma 5.2 *Let $m \geq 1$ and $A \geq 1$ be integers, and $b \in \mathbb{R}$. For any real number $U > 0$, we have*

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

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

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

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

Proof See [6]. ∎

5.2 Gauss Sums

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

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

In this section, we recall one classic result on Gauss sums:

Theorem 5.3 *For all $(a, b, m) \in \mathbb{Z}^3$ with $m \geq 1$, $\big|\sum_{n=0}^{m-1} \mathrm{e}(\frac{an^2+bn}{m})\big| \leq \sqrt{2m \gcd(a, m)}$ holds.*

Proof This form was obtained from [12, Proposition 2]. ∎

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

Lemma 5.4 *For all $(a, b, m, N, n_0) \in \mathbb{Z}^5$ with $m \geq 1$ and $N \geq 0$, we have*

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

Proof This is Lemma 9 of [6]. ∎

5.3 Carry Lemmas

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

Lemma 5.5 *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, we find for any block-additive function b that the number of integers $n < q^\nu$ with*

$$b_{\lambda-m+1}((n+r)^2) - b_{\lambda-m+1}(n^2) \neq b((n+r)^2) - b(n^2)$$

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

Proof A proof for the Thue–Morse sequence can be found in [6] and it is easy to adapt it for this more general case. ∎

The next lemma helps us replace quadratic exponential sums depending only on a few digits.

Lemma 5.6 *Let* $(\lambda,\mu,\nu,\rho') \in \mathbb{N}^4$ *such that* $0<\mu<\nu<\lambda$, $2\rho' \le \mu \le \nu-\rho'$, *and* $\lambda-\nu \le 2(\mu-\rho')$, *and set* $\mu' = \mu-\rho'$. *For integers* $n<q^\nu$, $s\ge 1$ *and* $1\le r\le q^{(\lambda-\nu)/2}$ *we set*

$$\begin{aligned} n^2 &\equiv u_1 q^{\mu'} + w_1 \pmod{q^{\lambda+m-1}}, && (0\le w_1 < q^{\mu'},\ 0\le u_1 < q^{\lambda+m-1-\mu+\rho'}),\\ (n+r)^2 &\equiv u_2 q^{\mu'} + w_2 \pmod{q^{\lambda+m-1}}, && (0\le w_2 < q^{\mu'},\ 0\le u_2 < q^{\lambda+m-1-\mu+\rho'}),\\ 2n &\equiv u_3 q^{\mu'} + w_3 \pmod{q^{\lambda+m-1}}, && (0\le w_3 < q^{\mu'},\ 0\le u_3 < q^{\nu+1-\mu+\rho'}),\\ 2sq^{m-1}n &\equiv v \pmod{q^{\lambda-\mu+m-1}}, && (0\le v < q^{\lambda-\mu+m-1}), \end{aligned}$$

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* $\ell\ge 1$ *the number of integers* $n<q^\nu$ *for which one of the following conditions*

$$\begin{gathered} b_{\mu,\lambda}((n+\ell)^2) \ne b_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3),\\ b_{\mu,\lambda}((n+\ell+sq^{\mu+m-1})^2) \ne b_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+vq^{\rho'}+2\ell sq^{m-1}q^{\rho'}),\\ b_{\mu,\lambda}((n+r+\ell)^2) \ne b_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3),\\ b_{\mu,\lambda}((n+r+\ell+sq^{\mu+m-1})^2) \ne b_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3+vq^{\rho'}+2(\ell+r)sq^{m-1}q^{\rho'}), \end{gathered}$$

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

Proof A proof for the sum of digits function in base 2 can be found in [6] and it is straight forward to adapt it to fit this more general case. ∎

5.4 Van der Corput's Inequality

Lemma 5.7 ([12]) *For all complex numbers* $z_1,\dots,z_N$ *and all integers* $Q\ge 1$ *and* $R\ge 1$, *we have*

$$\Big|\sum_{n=1}^{N-1} z_n\Big|^2 \le \frac{N+QR-Q}{R}\Big(\sum_{n=1}^{N-1}|z_n|^2 + 2\sum_{r=1}^{R-1}\Big(1-\frac{r}{R}\Big)\sum_{n=1}^{N-Qr-1}\Re(z_{n+Qr}\overline{z_n})\Big),$$

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

5.5 Vaaler's Method

The following theorem, developed by Vaaler [21], gives a classical method for detecting real numbers in an interval modulo 1 by means of exponential sums. For $\alpha\in\mathbb{R}$ with $0\le\alpha<1$, we denote by χ_α the characteristic function of the interval $[0,\alpha)$

modulo 1,

$$\chi_\alpha(x) = \lfloor x \rfloor - \lfloor x - \alpha \rfloor. \tag{5.2}$$

The following theorem is a consequence of Vaaler [21]. The presented form was first published by Mauduit and Rivat [13].

Theorem 5.8 *For all $\alpha \in \mathbb{R}$ with $0 \le \alpha < 1$ and all integer $H \ge 1$, there exist real-valued trigonometric polynomials $A_{\alpha,H}(x)$ and $B_{\alpha,H}(x)$ such that for all $x \in \mathbb{R}$*

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

The trigonometric polynomials are defined by

$$A_{\alpha,H}(x) = \sum_{|h|\le H} a_h(\alpha,H)\,\mathrm{e}(hx),\; B_{\alpha,H}(x) = \sum_{|h|\le H} b_h(\alpha,H)\,\mathrm{e}(hx), \tag{5.3}$$

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

$$a_0(\alpha,H) = \alpha, |a_h(\alpha,H)| \le \min\Big(\alpha, \frac{1}{\pi|h|}\Big), \quad |b_h(\alpha,H)| \le \frac{1}{H+1}.$$

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

Lemma 5.9 *For $(\alpha_1,\dots,\alpha_d) \in [0,1)^d$ and $(H_1,\dots,H_d) \in \mathbb{N}^d$ with $H_1 \ge 1,\dots,H_d \ge 1$, we have for all $(x_1,\dots,x_d) \in \mathbb{R}^d$*

$$\Big|\prod_{j=1}^{d} \chi_{\alpha_j}(x_j) - \prod_{j=1}^{d} A_{\alpha_j,H_j}(x_j)\Big| \le \sum_{\emptyset \ne J \subseteq \{1,\dots,d\}} \prod_{j \notin J} \chi_{\alpha_j}(x_j) \prod_{j \in J} B_{\alpha_j,H_j}(x_j),$$

where $A_{\alpha,H}(\cdot)$ and $B_{\alpha,H}(\cdot)$ are the real valued trigonometric polynomials defined by (5.3).

Proof See [13]. ■

Let $(U_1,\dots,U_d) \in \mathbb{N}^d$ with $U_1 \ge 1,\dots,U_d \ge 1$ and define $\alpha_1 = 1/U_1,\dots,\alpha_d = 1/U_d$. For $j = 1,\dots,d$ and $x \in \mathbb{R}$, we have $\sum_{0 \le u_j < U_j} \chi_{\alpha_j}\big(x - \frac{u_j}{U_j}\big) = 1$. Let $N \in \mathbb{N}$ with $N \ge 1$, $f\colon \{1,\dots,N\} \to \mathbb{R}^d$, and $g\colon \{1,\dots,N\} \to \mathbb{C}$ such that $|g| \le 1$. If $f = (f_1,\dots,f_d)$, we can express the sum $S = \sum_{n=1}^{N} g(n)$ as

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

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

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

https://doi.org/10.4153/CJM-2017-053-1 Published online by Cambridge University Press

Lemma 5.10 *With the notations from above, we have*

$$|S - \widetilde{S}| \le \sum_{\ell=1}^{d-1} \sum_{1\le j_1<\cdots<j_\ell} \frac{U_{j_1}\cdots U_{j_\ell}}{H_{j_1}\cdots H_{j_\ell}} \sum_{|h_{j_1}|\le H_{j_1}/U_{j_1}} \cdots \sum_{|h_{j_\ell}|\le H_{j_\ell}/U_{j_\ell}} \Big| \sum_{n=1}^{N} \mathrm{e}(h_{j_1} U_{j_1} f_{j_1}(n) + \cdots + h_{j_\ell} U_{j_\ell} f_{j_\ell}(n)) \Big|. \tag{5.4}$$

Proof See [13]. ∎

References

[1] J.-P. Allouche and J. Shallit, *Automatic sequences*. Cambridge, Cambridge University Press, 2003.
[2] V. Becher, P. A. Heiber, and T. A. Slaman, *A polynomial-time algorithm for computing absolutely normal numbers*. Inform. and Comput. **232**(2013), 1–9. http://dx.doi.org/10.1016/j.ic.2013.08.013
[3] R. Bellman and H. N. Shapiro, *On a problem in additive number theory*. Ann. of Math. (2) **49**(1948, 333–340. http://dx.doi.org/10.2307/1969281
[4] Y. Bugeaud, *Distribution modulo one and Diophantine approximation*. Cambridge Tracts in Mathematics, 193. Cambridge University Press, Cambridge, 2012.
[5] E. Cateland, *Suites digitales et suites k-régulières*. Ph.D. thesis, Université Bordeaux I, 1992.
[6] M. Drmota, C. Mauduit, and J. Rivat, *The Thue-Morse sequence along squares is normal*. http://www.dmg.tuwien.ac.at/drmota/alongsquares.pdf
[7] S. Ferenczi, *Complexity of sequences and dynamical systems*. Discrete Math. **206**(1999), no. 1–3, 145–154. http://dx.doi.org/10.1016/S0012-365X(98)00400-2
[8] N. P. Fogg, *Substitutions in dynamics, arithmetics and combinatorics*. Lecture Notes in Mathematics, 1794. Springer-Verlag, Berlin, 2002.
[9] A. O. Gel'fond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*. Acta Arith. **13**(1967/1968), 259–265.
[10] P. Kurka, *Topological and symbolic dynamics*. Cours Spécialisés, 11. Société Mathématique de France, Paris, 2003.
[11] M. B. Levin, *Absolutely normal numbers*. Vestnik Moskov. Univ. Ser. I Mat. Mekh. (1979), no. 1, 31–37, 87.
[12] C. Mauduit and J. Rivat, *La somme des chiffres des carrés*. Acta Math. **203**(2009), no. 1, 107–148. http://dx.doi.org/10.1007/s11511-009-0040-0
[13] ———, *Prime numbers along Rudin-Shapiro sequences*. J. Eur. Math. Soc. (JEMS) **17**(2015), no. 10, 2595–2642. http://dx.doi.org/10.4171/JEMS/566
[14] M. Mendès France, *Nombres normaux. Applications aux fonctions pseudo-aléatoires*. J. Analyse Math. **20**(1967), 1–56.
[15] Y. Moshe, *On the subword complexity of Thue-Morse polynomial extractions*. Theoret. Comput. Sci. **389**(2007), no. 1–2, 318–329. http://dx.doi.org/10.1016/j.tcs.2007.10.015
[16] M. Queffélec, *Substitution dynamical systems–spectral analysis*. Second edition. Lecture Notes in Mathematics, 1294. Springer-Verlag, Berlin, 2010.
[17] A.-M. Scheerer, *Computable absolutely normal numbers and discrepancies*. Math. Comp. **86**(2017), no. 308, 2911–2926. http://dx.doi.org/10.1090/mcom/3189
[18] W. M. Schmidt, *Über die Normalität von Zahlen zu verschiedenen Basen*. Acta Arith. **7**(1961/1962), 299–309. http://dx.doi.org/10.4064/aa-7-3-299-309
[19] W. Sierpinski, *Démonstration élémentaire du théorème de M. Borel sur les nombres absolument normaux et détermination effective d'une tel nombre*. Bull. Soc. Math. France **45**(1917), 125–132. http://dx.doi.org/10.24033/bsmf.977
[20] A. Turing and P. Saunders, *Collected Works of A. M. Turing*. North-Holland, Amsterdam, 1992.
[21] J. D. Vaaler, *Some extremal functions in Fourier analysis*. Bull. Amer. Math. Soc. (N.S.) **12**(1985), no. 2, 183–216., 1985. http://dx.doi.org/10.1090/S0273-0979-1985-15349-2

Institut für Diskrete Mathematik und Geometrie TU Wien, Wiedner Hauptstr. 8-10, 1040 Wien, Austria
e-mail: clemens.muellner@tuwien.ac.at