NORMALITY ALONG SQUARES

MICHAEL DRMOTA, CHRISTIAN MAUDUIT, AND JOËL RIVAT

Abstract. The goal of this work is to show a first example of an almost periodic zero entropy sequence (in the sense of symbolic dynamical systems) whose subsequence along squares is a normal sequence. As an application, this provides a new method to produce normal numbers in a given base.

1. Introduction

The study of subsequences along squares or along integer valued polynomials induced a lot of interest since the questions asked by Bellow [2] and Furstenberg [14] and the proof by Bourgain of a pointwise ergodic theorem in [5, 6, 7] (see also [3], [9], [16], [17], [29] for other important results in this direction). The goal of this work is to give an explicit example of an almost periodic sequence with zero entropy (the Thue-Morse sequence) which subsequence along squares is normal. This surprising result is optimal in the following sense:

- the Thue-Morse sequence is one of the simplest example of non periodic sequence on two symbols (and we can't expect a similar normality result starting from a periodic sequence);
- the sequence of squares is one of the simplest slowly increasing sequence of integers if we except arithmetic progressions (and we can't expect such a normality result by extracting arithmetic progressions).

In this paper we denote by $\mathbb{N}$ the set of non negative integers, by $\mathbb{U}$ the set of complex numbers of modulus 1 and we set $\mathrm{e}(x) = \exp(2i\pi x)$ for any real number x. If f and g are two functions such that there exist $C > 0$ with $|f| \le C\, g$ we write $f = O(g)$ or $f \ll g$.

1.1. The Thue-Morse dynamical system.

Let $(\mathbf{t}_r)_{r\in\mathbb{N}}$ and $(\mathbf{t}'_r)_{r\in\mathbb{N}}$ be the sequences of words on the alphabet $\{0,1\}$ defined by

$$\mathbf{t}_0 = 0,\ \mathbf{t}'_0 = 1,\ \mathbf{t}_{r+1} = \mathbf{t}_r\mathbf{t}'_r,\ \text{and}\ \mathbf{t}'_{r+1} = \mathbf{t}'_r\mathbf{t}_r$$

(in all this paper we identify words $b_0 \dots b_{k-1}$ on the alphabet $\{0,1\}$ with sequences $(b_i)_{i\in\{0,\dots,k-1\}} \in \{0,1\}^k$ and we denote by UV the concatenation of the words U and V on the alphabet $\{0,1\}$). The sequence $(\mathbf{t}_r)_{r\in\mathbb{N}}$ converges for the product topology in $\{0,1\}^{\mathbb{N}}$ to an infinite word $\mathbf{t} \in \{0,1\}^{\mathbb{N}}$ called the Thue-Morse sequence (or Thue-Morse infinite word).

There are many other ways to define the Thue-Morse sequence $\mathbf{t} = (t(n))_{n\in\mathbb{N}} \in \{0,1\}^{\mathbb{N}}$. In particular it is easy to check that, for any non negative integer n, we have

$$t(n) = \mathrm{s}(n) \bmod 2$$

where $\mathrm{s}(n)$ denotes the number of powers of 2 in the binary representation of n. Since its introduction independently by Thue in [27] and by Morse in [23], the Thue-Morse sequence has been studied in many different contexts from combinatorics to algebra, number theory, harmonic analysis, ergodic theory, geometry and dynamical systems (see [1, 19]).

Date: June 14, 2017.

2010 *Mathematics Subject Classification.* Primary: 11A63, 11B85, 11K16, Secondary: 11L07, 37B10.

Key words and phrases. Normal sequences, Thue-Morse sequence, exponential sums, correlation.

This work was supported by the Agence Nationale de la Recherche project ANR-14-CE34-0009 MUDERA and by the FWF-Project S55-02 "Subsequences of Automatic Sequences and Uniform Distribution".

Definition 1. *The symbolic dynamical system associated to a sequence* $\mathbf{u} \in \{0,1\}^{\mathbb{N}}$ *is the system* $(X(\mathbf{u}), T)$*, where* T *is the shift on* $\{0,1\}^{\mathbb{N}}$ *and* $X(\mathbf{u})$ *the closure (for the product topology of* $\{0,1\}^{\mathbb{N}}$*) of the orbit of* $\mathbf{u}$ *under the action of* T*.*

We say that $(b_0, \dots, b_{k-1}) \in \{0,1\}^k$ is a factor of the sequence $\mathbf{u} \in \{0,1\}^{\mathbb{N}}$ if there exists an integer i such that $u(i) = b_0, \dots, u(i+k-1) = b_{k-1}$.

Definition 2. *A sequence* $\mathbf{u} \in \{0,1\}^{\mathbb{N}}$ *is almost periodic (or uniformly recurrent) if every factor of* $\mathbf{u}$ *occurs infinitely often in* $\mathbf{u}$ *with bounded gaps.*

Morse proved in [23] that $\mathbf{t}$ is an almost periodic sequence (see also [19, Proposition 4] or [25, Proposition 5.1.2]). This property means that the dynamical system $(X(\mathbf{t}), T)$ is minimal (*i.e.* the only closed T-invariant sets in $X(\mathbf{t})$ are $\emptyset$ and $X(\mathbf{t})$, see [26, Theorem IV.12] or [25, Proposition 5.1.13]).

Remark 1. *It follows from a result of Gottschalk and Hedlund (see* [15]*) that* $X(\mathbf{t})$ *is exactly the set of non overlapping binary sequences* i.e. *the set of sequences* $\mathbf{u} \in \{0,1\}^{\mathbb{N}}$ *with no factor of the form* BBb *where* b *is the first element of* B*.*

1.2. Low complexity of the Thue-Morse sequence.

Definition 3. *For any integer* $q \geq 2$*, the symbolic complexity of a sequence* $\mathbf{u} \in \{0, \dots, q-1\}^{\mathbb{N}}$ *is the function* $p_{\mathbf{u}}$ *defined for any positive integer* k *by*

$$p_{\mathbf{u}}(k) = \operatorname{card}\{(b_0, \dots, b_{k-1}) \in \{0, \dots, q-1\}^k,\ \exists i \,/\, u(i) = b_0, \dots, u(i+k-1) = b_{k-1}\}$$

*(*i.e. $p_{\mathbf{u}}(k)$ *is equal to the number of distinct factors of length* k *that occur in the sequence* $\mathbf{u}$*).*

The function $p_{\mathbf{u}}$ constitutes a possible measure for the pseudorandomness of the sequence $\mathbf{u}$. More precisely, it is easy to show that the topological entropy of the symbolic dynamical system $(X(\mathbf{u}), T)$ is equal to $\lim_{k\to\infty} \frac{\log p_{\mathbf{u}}(k)}{k}$ (see [18]).

The symbolic complexity of the sequence $\mathbf{t}$ is very low: it follows from [8, Proposition 4.5] or [13, Corollary 4.5] that for any positive integer k we have $p_{\mathbf{t}}(k) \leq \frac{10}{3}k$. For any fixed $(a,b) \in \mathbb{N}^2$ it is easy the check that the sequence $\mathbf{t}_{a,b} = (t(an+b))_{n\in\mathbb{N}}$ is also obtained by a simple algorithm. More precisely $\mathbf{t}_{a,b}$ is generated by a finite 2-automaton (see [1] for a definition of this notion). It follows that the combinatorial structure of the sequence $\mathbf{t}_{a,b}$ can be understood from the study of its associated 2-automaton and that its symbolic complexity is also sublinear: $p_{\mathbf{t}_{a,b}}(k) = O_a(k)$ (see [12, Theorem 2]). This shows that any symbolic dynamical system $(X(\mathbf{t}_{a,b}), T)$ obtained by extracting a subsequence of $\mathbf{t}$ along arithmetic progressions still has zero topological entropy.

1.3. Main result.

The goal of this work is to show that the situation changes completely when we replace linear subsequences by quadratic ones.

Definition 4. *A sequence* $\mathbf{u} \in \{0, \dots, q-1\}^{\mathbb{N}}$ *is normal if, for any* $k \in \mathbb{N}$ *and any* $(b_0, \dots, b_{k-1}) \in \{0, \dots, q-1\}^k$*, we have*

$$\lim_{N\to\infty} \frac{1}{N} \operatorname{card}\{i < N,\ u(i) = b_0, \dots, u(i+k-1) = b_{k-1}\} = \frac{1}{q^k}.$$

It follows from Definition 4 that if $\mathbf{u} \in \{0, \dots, q-1\}^{\mathbb{N}}$ is normal then every factor occurs in the sequence $\mathbf{u}$ so that, for any non negative integer k, we have $p_{\mathbf{u}}(k) = q^k$ and the topological entropy of $(X(\mathbf{u}), T)$ is equal to $\log q$. But the converse is not true: normality is a much stronger property than maximal topological entropy.

Moshe proved in [24] that every factor occurs in the sequence $\mathbf{t_2}$ answering a question due to Allouche and Shallit [1, Problem 10.12.7] but his method does not provide any information about the frequency of occurency of a given factor, which constitute a much more difficult problem.

Theorem 1. *The sequence* $\mathbf{t_2} = (t(n^2))_{n\in\mathbb{N}}$ *is normal.*

Definition 5. *For any integer* $q \geq 2$*, a real number is normal in base* q *if the sequence of its* q*-adic digits is normal.*

The notion of normal number in a given base was introduced by Borel in [4]. The first explicit construction was given by Champernowne in [11] and only few such constructions are known (see [10, Chapters 4 and 5]). This theorem provides a new method to construct normal numbers in a given base.

Corollary 1. *The real number* $\alpha = \sum_{n=0}^{\infty} \frac{t(n^2)}{2^n}$ *is normal in base* 2*.*

Remark 2. *For any integer* $q \geq 2$*, a generalized Thue-Morse sequence* $\mathbf{t}^{(q)} \in \{0, \dots, q-1\}^{\mathbb{N}}$ *can be defined by*

$$\forall n \in \mathbb{N},\ t^{(q)}(n) = \mathrm{s}(n) \bmod q.$$

Our method might be adapted to prove that $\mathbf{t}^{(q)}$ *is normal, providing an example of a real number normal in base* q*:* $\alpha^{(q)} = \sum_{n=0}^{\infty} \frac{t^{(q)}(n^2)}{q^n}$*.*

Remark 3. *Our proof works (with some extra technicity) if we replace* n^2 *by any quadratic polynomial taking values in* $\mathbb{N}$*.*

If we replace n^2 by $P(n)$ where P is a polynomial of degree ≥ 3 taking values in $\mathbb{N}$ it is still an open problem to determine the frequency of 0 and 1 in the sequence $(t(P(n)))_{n\in\mathbb{N}}$. But we believe that the following much stronger conjecture is true:

Conjecture 1. *For any polynomial* P *of degree* ≥ 3 *taking values in* $\mathbb{N}$ *the sequence* $(t(P(n)))_{n\in\mathbb{N}}$ *is normal.*

If we replace n^2 by p_n (the n-th prime number) Mauduit and Rivat proved in [21] that the frequencies of 0 and 1 in the sequence $(t(p_n))_{n\in\mathbb{N}}$ are both equal to $\frac{1}{2}$. It seems out of reach to determine the frequencies of 00, 01, 10 and 11 in this sequence, but we believe that the following conjecture is true:

Conjecture 2. *The sequence* $(t(p_n))_{n\in\mathbb{N}}$ *is normal.*

2. Plan of the Proof

2.1. **Introduction of exponential sums.** For any $(b_0, \dots, b_{k-1}) \in \{0,1\}^k$ we have

$$\begin{aligned}
&\mathrm{card}\{n < N : (t_{n^2}, \dots, t_{(n+k-1)^2}) = (b_0, \dots, b_{k-1})\} \\
&= \sum_{n<N} \frac{1}{2} \sum_{\alpha_0=0}^{1} \mathrm{e}\left(\frac{\alpha_0}{2}\left(\mathrm{s}(n^2) - b_0\right)\right) \cdots \frac{1}{2} \sum_{\alpha_{k-1}=0}^{1} \mathrm{e}\left(\frac{\alpha_{k-1}}{2}\left(\mathrm{s}((n+k-1)^2) - b_{k-1}\right)\right) \\
&= \frac{1}{2^k} \sum_{(\alpha_0,\dots,\alpha_{k-1})\in\{0,1\}^k} \mathrm{e}\left(-\frac{\alpha_0 b_0 + \cdots + \alpha_{k-1} b_{k-1}}{2}\right) \sum_{n<N} \mathrm{e}\left(\frac{1}{2}\sum_{\ell=0}^{k-1} \alpha_\ell\, \mathrm{s}((n+\ell)^2)\right) \\
&= \frac{N}{2^k} + \frac{1}{2^k} O\left(\sum_{(\alpha_0,\dots,\alpha_{k-1})\in\{0,1\}^k\setminus\{(0,\dots,0)\}} \left|\sum_{n<N} \mathrm{e}\left(\frac{1}{2}\sum_{\ell=0}^{k-1} \alpha_\ell\, \mathrm{s}((n+\ell)^2)\right)\right|\right).
\end{aligned}$$

It follows that in order to prove Theorem 1 it is enough to prove the following theorem on exponential sums.

Theorem 2. *For any integer $k \geq 1$ and $(\alpha_0, \dots, \alpha_{k-1}) \in \{0,1\}^k$ such that $(\alpha_0, \dots, \alpha_{k-1}) \neq (0, \dots, 0)$, there exists $\eta > 0$ such that*

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

Remark 4. *It follows from our method that the same estimate remains valid for the sums $\sum_{n<N} \mathrm{e}\left(\frac{1}{2}\sum_{\ell=0}^{k-1} \alpha_\ell \, \mathrm{s}(m+(n+\ell)^2)\right)$ uniformly for $m \in \mathbb{N}$, so that Theorem 1 still holds for any sequence of $X(\mathbf{t})$:*

The following result is a consequence of Theorem 1, Remark 1 and Remark 4:

Theorem 3. *If $\mathbf{u}$ is a non overlapping binary sequence then the sequence $(u(n^2))_{n\in\mathbb{N}}$ is normal.*

2.2. **Strategy of the proof of Theorem 2.** The case $k = 1$ follows from [20], but the method used in [20] fails when $k \geq 2$ for many reasons (the first of them being the huge size and the large number of variables in the exponential sums) and leads us to introduce a new approach in order to be able to control the Fourier transform of correlations of any order.

First we use a multidimensional approximation method (of Beurling-Selberg-Vaaler type, see section 9.1) which produces exponential sums much shorter than in [20]. Then the method used in [20] to detect the squares would lead to introduce a huge number of variables ($4k$) in these exponential sums and the next idea is to reduce this number to a constant independent of k at the price of Fourier transform terms much more difficult to handle. Then the control of these Fourier transform terms leads to estimate norms of products of large matrices (of size depending on k). These estimates constitute the most difficult part of the proof and require a new strategy. In order to obtain these upper bounds we introduce a method based on combinatorial arguments for families of weighted graphs associated to these matrices.

Let us describe more precisely the structure of the full proof of Theorem 2. Section 3 is devoted to some properties of the carry propagation (in particular we have to provide a quantitative statement of the fact that carry propagation along several digits are rare). The main ingredients of the proof of Theorem 2 are upper bounds on the Fourier terms $G_\lambda^I(h,d)$ defined in section 4 by (7). The other ingredients include Van-der-Corput type inequalities in order to reduce the problem to sums that depend only on few digits of $n^2, (n+1)^2, \dots, (n+k-1)^2$. These reduced sums have a periodic structure that allows a proper Fourier analytic treatment. After the Fourier analysis the problem is roughly speaking split into a part where the Fourier terms $G_\lambda^I(h,d)$ appear and into a second part involving quadratic Gauss sums. The bounds corresponding to the Fourier terms are formulated in Propositions 1 and 2 (see Section 4) and proved in Sections 7 and 8. We have to distinguish in the proof of Theorem 2 between the cases where $K = \alpha_0 + \cdots + \alpha_{k-1}$ is even and where K is odd, and Sections 5 and 6 correspond to this distinction. In Section 5 we prove that if K is even we can deduce Theorem 2 from Proposition 1 and in Section 6 we prove that if K is odd we can deduce Theorem 2 from Proposition 2. Finally, the next two sections (Sections 7 and 8) provide the proofs of Propositions 1 and 2. Proposition 1 is a bound on averages of Fourier transforms while Proposition 2 is a uniform bound much more difficult to obtain. Section 9 contains useful technical results on exponential sums, quadratic Gauss sums and norms of matrix products.

3. Truncated functions and carry Lemmas

Let $\varepsilon_j(n) \in \{0,1\}$ denote the j-th digit in the binary representation of a non-negative integer n and write

$$f(n) = \frac{1}{2}\,\mathrm{s}(n) = \frac{1}{2}\sum_{j\geq 0} \varepsilon_j(n).$$

For $(\lambda,\mu)\in\mathbb{N}^2$ such that $0\le\mu<\lambda$, we define the truncated function f_λ and the two-fold truncated function $f_{\mu,\lambda}$ by

$$f_\lambda(n)=\frac{1}{2}\sum_{0\le j<\lambda}\varepsilon_j(n)\quad\text{and}\quad f_{\mu,\lambda}(n)=\frac{1}{2}\sum_{\mu\le j<\lambda}\varepsilon_j(n)=f_\lambda(n)-f_\mu(n).$$

Lemma 1. *Let $(\nu,\lambda,\rho)\in\mathbb{N}^3$ such that $\nu+\rho\le\lambda\le 2\nu$. For any integer r with $0\le r\le 2^\rho$ the number of integers $n<2^\nu$ for which there exists an integer $j\ge\lambda$ with $\varepsilon_j((n+r)^2)\ne\varepsilon_j(n^2)$ is $\ll 2^{2\nu+\rho-\lambda}$. Hence, the number of integers $n<2^\nu$ with*

$$f_\lambda((n+r)^2)-f_\lambda(n^2)\ne f((n+r)^2)-f(n^2)$$

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

Proof. It is sufficient to adapt the proof of Lemma 16 of [20] taking λ in place of $\nu+2\rho+1$. □

Lemma 2. *Let $(\lambda,\mu,\nu,\mu',\rho')\in\mathbb{N}^5$ such that $0<\mu<\nu<\lambda\le 2\mu$, $\rho'\ge 3$, $\mu'=\mu-\rho'$, $2\rho'\le\mu\le\nu-\rho'$ and $\lambda-\nu\le 2(\mu-\rho')$. For any integers $n<2^\nu$, $s\ge 1$ and $1\le r\le 2^{(\lambda-\nu)/2}$ we define 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 $w_3=w_3(n)$ by the following conditions:*

$$\begin{aligned}
n^2&\equiv u_1 2^{\mu'}+w_1 \bmod 2^\lambda && (0\le w_1<2^{\mu'},\ 0\le u_1<U_1)\\
(n+r)^2&\equiv u_2 2^{\mu'}+w_2 \bmod 2^\lambda && (0\le w_2<2^{\mu'},\ 0\le u_2<U_2)\\
2n&\equiv u_3 2^{\mu'}+w_3 \bmod 2^\lambda && (0\le w_3<2^{\mu'},\ 0\le u_3<U_3)\\
2sn&\equiv v \bmod 2^{\lambda-\mu}, && (0\le v<V),
\end{aligned}\tag{2}$$

where

$$U_1=U_2=2^{\lambda-\mu'},\ U_3=2^{\nu+1-\mu'},\ V=2^{\lambda-\mu}.\tag{3}$$

Then, uniformly for integers ℓ such that $1\le\ell\le 2^{\mu'-3}$, the number of integers $n<2^\nu$ for which at least one of the following conditions

$$\begin{aligned}
f_{\mu,\lambda}((n+\ell)^2)&\ne f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3)\\
f_{\mu,\lambda}((n+\ell+s2^\mu)^2)&\ne f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+v2^{\rho'}+\ell s2^{\rho'+1})\\
f_{\mu,\lambda}((n+r+\ell)^2)&\ne f_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3)\\
f_{\mu,\lambda}((n+r+\ell+s2^\mu)^2)&\ne f_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3+v2^{\rho'}+(\ell+r)s2^{\rho'+1})
\end{aligned}\tag{4}$$

is satisfied is $\ll 2^{\nu-\rho'}$.

Proof. We first consider the case $(n+\ell)^2$. The other cases are similar and we will comment on them at the end of the proof. We have

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

This means that if $w_1+\ell w_3+\ell^2<2^{\mu'}$ then for $0\le j<\lambda-\mu'$ we have $\varepsilon_{\mu'+j}((n+\ell)^2)=\varepsilon_j(u_1+\ell u_3)$. However, if $w_1+\ell w_3+\ell^2\ge 2^{\mu'}$ then there is a carry propagation. However, we will show that there are only few exceptions where more than ρ' digits are changed. More precisely the proof is split into the following two steps:

(1) If the digits block $(\varepsilon_j((n+\ell)^2))_{\mu\le j<\lambda}$ differ from the digits block $(\varepsilon_j(u_1+\ell u_3))_{\rho'\le j<\lambda-\mu+\rho'}$, where $u_1=u_1(n)$ and $u_3=u_3(n)$ are defined in (2), then we have

$$\frac{(n+\ell)^2}{2^\mu}-\left\lfloor\frac{(n+\ell)^2}{2^\mu}\right\rfloor\le\alpha\quad\text{or}\quad\frac{(n+\ell)^2}{2^\mu}-\left\lfloor\frac{(n+\ell)^2}{2^\mu}\right\rfloor\ge 1-\alpha,\tag{5}$$

where $0<\alpha<1$ will be independent of ℓ.

(2) The number of integers $n < 2^\nu$ with (5) is $\ll 2^{\nu-\rho'}$.

Of course if these two properties are true then Lemma 2 is proven.

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

$$\tilde{w} := \left\lfloor 2^{-\mu'} \left(w_1 + \ell w_3 + \ell^2 \right) \right\rfloor \le D := \left\lfloor 2^{-\mu'} \left(2^{\mu'} + 2^{2\mu'-3} + 2^{2\mu'-6} \right) \right\rfloor$$

can only attain values in $\{0, 1, 2, \dots, D\}$. These values of $\tilde{w}$ will certainly affect some of (lower order) digits of $u_1 + \ell u_3$. Let $\tilde{v} := u_1 + \ell u_3 \bmod 2^{\rho'}$ with $0 \le \tilde{v} < 2^{\rho'}$. Then the digits $\varepsilon_j(u_1 + \ell u_3)$, $\rho' \le j < \lambda - \mu'$, might be affected by this carry if $\tilde{v} \in \{2^{\rho'} - 1, 2^{\rho'} - 2, \dots, 2^{\rho'} - D\}$. Now since

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

it immediately follows that (5) holds with $0 < \alpha = (D+1)\, 2^{-\mu} < 1$. This completes the proof of the first part.

Let χ_α denote the characteristic function of the interval $[0, \alpha)$ modulo 1:

$$\chi_\alpha(x) = \lfloor x \rfloor - \lfloor x - \alpha \rfloor . \tag{6}$$

Next let Z denote the number integers of $n < 2^\nu$ with (5). We may write

$$Z = \sum_{n<2^\nu} \left(\chi_\alpha \left(2^{-\mu}(n+\ell)^2 \right) + \chi_\alpha \left(-2^{-\mu}(n+\ell)^2 \right) \right).$$

Then by Lemma 9 we have

$$Z \le 2 \sum_{|h|\le H} \left(\alpha + \frac{1}{H} \right) \left| \sum_{n<2^\nu} \mathrm{e}\left(h \frac{(n+\ell)^2}{2^\mu} \right) \right|$$

and we can set $H = 2^{\rho'}$. It is clear that the main contribution comes from the term with $h = 0$ which gives an upper bound of the form $O(2^{\nu-\rho'})$. Now every $h \ne 0$ with $|h| \le H = 2^{\rho'}$ can be written as $h = h'2^t$, where $0 \le t \le \rho'$ and h' is odd with $|h'| \le 2^{\rho'-t}$. Then we have by Lemma 16

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

and consequently

$$\begin{aligned} 2^{-\rho'} \sum_{0\ne|h|\le 2^{\rho'}} \left| \sum_{n<2^\nu} \mathrm{e}\left(h \frac{(n+\ell)^2}{2^\mu} \right) \right| &\ll 2^{-\rho'} \sum_{0\le t\le\rho'} 2^{\rho'-t} \left(2^{\nu+(t-\mu)/2} + \mu 2^{(\mu+t)/2} \right) \\ &\ll 2^{\nu-\mu/2} + \mu 2^{\mu/2}. \end{aligned}$$

Since $\mu \ll 2^{\mu/2}$ and $2\rho' \le \mu \le \nu - \rho'$ all contributions are $\ll 2^{\nu-\rho'}$. This completes the proof of the second part.

Finally we comment on the other cases. First, there is no change for $(n + \ell + s2^\mu)^2$ since $\lambda \le 2\mu$ implies that the term $s2^\mu$ does not affect the discussed carry propagation. Next we have

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

Observing that $1 \le r \le 2^{\mu'}$ we have

$$2^{-\mu'}(w_2 + \ell w_3 + \ell^2 + 2r\ell) \le 2^{-\mu'} \left(2^{\mu'} + 2^{2\mu'-3} + 2^{2\mu'-6} + 2^{2\mu'-2} \right)$$

which ensures that $0 < \alpha < 1$. The same argument applies for the final case $(n + \ell + s2^\mu + r)^2$. □

4. Fourier estimates

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

$$G_\lambda^I(h,d) = \frac{1}{2^\lambda} \sum_{0 \le u < 2^\lambda} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell f_\lambda(u + \ell d + i_\ell) - hu2^{-\lambda} \right), \tag{7}$$

where $\alpha_\ell \in \{0,1\}$ (we assume that $\alpha_0 = 1$). This sum can be also seen as the discrete Fourier transform of the function

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

For any $I \in \mathcal{I}_k$ we define

$$|I| = \alpha_0 i_0 + \cdots + \alpha_{k-1} i_{k-1},\ K = \alpha_0 + \cdots + \alpha_{k-1} \text{ and } \sigma = \sum_{\ell=0}^{k-1} \alpha_\ell \ell.$$

We start with a recurrence for the discrete Fourier transform terms $G_\lambda^I(h,d)$ defined by (7). For this purpose we define for any $(\varepsilon, \varepsilon') \in \{0,1\}^2$ the transformations on $\mathcal{I}_k$ defined for any $I = (i_0, i_1, \dots, i_{k-1}) \in \mathcal{I}_k$ by

$$T_{\varepsilon\varepsilon'}(I) = \left(\left\lfloor \frac{i_\ell + \ell\varepsilon + \varepsilon'}{2} \right\rfloor \right)_{\ell \in \{0,\dots,k-1\}}.$$

Lemma 3. *For any $I \in \mathcal{I}_k$, $h \in \mathbb{Z}$, $(d,\lambda) \in \mathbb{N}^2$ and $\varepsilon \in \{0,1\}$ we have*

$$G_\lambda^I(h, 2d+\varepsilon) = \frac{(-1)^{|I|+\sigma\varepsilon}}{2} G_{\lambda-1}^{T_{\varepsilon 0}(I)}(h,d) + \frac{(-1)^{|I|+K+\sigma\varepsilon}\,\mathrm{e}(-h/2^\lambda)}{2} G_{\lambda-1}^{T_{\varepsilon 1}(I)}(h,d). \tag{8}$$

Proof. We split up the sum $0 \le u < 2^\lambda$ into even and odd numbers and obtain for any $\varepsilon \in \{0,1\}$

$$\begin{aligned}
G_\lambda^I(h,2d+\varepsilon) =& \frac{1}{2^\lambda} \sum_{0 \le u < 2^{\lambda-1}} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell f_\lambda(2u + 2\ell d + \ell\varepsilon + i_\ell) - 2hu2^{-\lambda} \right) \\
&+ \frac{1}{2^\lambda} \sum_{0 \le u < 2^{\lambda-1}} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell f_\lambda(2u + 2\ell d + \ell\varepsilon + i_\ell + 1) - h(2u+1)2^{-\lambda} \right) \\
=& \frac{1}{2^\lambda} \sum_{0 \le u < 2^{\lambda-1}} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell \left(f_{\lambda-1}(u + \ell d + \lfloor (\ell\varepsilon + i_\ell)/2 \rfloor) + f(\varepsilon_0(\ell\varepsilon + i_\ell)) \right) - hu2^{-(\lambda-1)} \right) \\
&+ \frac{1}{2^\lambda} \sum_{0 \le u < 2^{\lambda-1}} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell \left(f_{\lambda-1}(u + \ell d + \lfloor (\ell\varepsilon + i_\ell + 1)/2 \rfloor) + f(\varepsilon_0(\ell\varepsilon + i_\ell + 1)) \right) \right. \\
&\qquad \left. - hu2^{-(\lambda-1)} - h2^{-\lambda} \right) \\
=& \frac{(-1)^{|I|+\sigma\varepsilon}}{2} G_{\lambda-1}^{T_{\varepsilon 0}(I)}(h,d) + \frac{(-1)^{|I|+K+\sigma\varepsilon}\,\mathrm{e}(-h/2^\lambda)}{2} G_{\lambda-1}^{T_{\varepsilon 1}(I)}(h,d),
\end{aligned}$$

since for any non negative integer i we have $\mathrm{e}(f(\varepsilon_0(i))) = \mathrm{e}(\frac{1}{2}(\varepsilon_0(i))) = (-1)^{\varepsilon_0(i)} = (-1)^i$. □

As $I \in \mathcal{I}_k$ implies that $(T_{00}(I), T_{01}(I), T_{10}(I), T_{11}(I)) \in \mathcal{I}_k^4$, it follows that the vector $\mathbf{G}_\lambda(h,d) = (G_\lambda^I(h,d))_{I\in\mathcal{I}_k}$ can be determined recursively.

The next two propositions are crucial for the proof of main result. Since the proofs are quite involved we postpone them to Sections 7 and 8.

Proposition 1. *If K is even, then there exists $\eta > 0$ such that for any $I \in \mathcal{I}_k$ we have*

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

uniformly for all integers h, where $\frac{1}{2}\lambda \le \lambda' \le \lambda$.

Proposition 2. *If K is odd, then there exists $\eta > 0$ such that for any $I \in \mathcal{I}_k$ we have*

$$\left|G_\lambda^I(h,d)\right| \ll 2^{-\eta L} \max_{J\in\mathcal{I}_k} \left|G_{\lambda-L}^J(h, \lfloor d/2^L \rfloor)\right|$$

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

5. The case K even

In this section we show that when $K = \alpha_0 + \cdots + \alpha_{k-1}$ is even, Proposition 1 provides an upper bound for the sum

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

Let ν be the unique integer such that

$$2^{\nu-1} < N \le 2^\nu$$

and let $(\lambda,\mu) \in \mathbb{N}^2$ such that

$$\mu < \nu < \lambda \text{ and } \lambda - \nu = \nu - \mu = \tfrac{1}{2}(\lambda-\mu) \tag{9}$$

(the precise values will be specified later).

By using Lemma 1 it follows that the number of integers $n < N$ such that the j-th digits of n^2, $(n+1)^2$, …, $(n+k-1)^2$ coincide for $j \ge \lambda$ is equal to $N - O(N2^{-(\lambda-\nu)})$. Furthermore since K is even it follows that we obtain for those n

$$\sum_{\ell=0}^{k-1} \alpha_\ell f_{\lambda,\infty}((n+\ell)^2) = f_{\lambda,\infty}(n^2)K \in \mathbb{Z},$$

where $f_{\lambda,\infty} = f - f_\lambda$ (notice that $2f_{\lambda,\infty}$ is integer valued). Consequently, if we set

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

then

$$S_0 = S_1 + O\left(2^{\nu-(\lambda-\nu)}\right). \tag{10}$$

Next we apply Lemma 12 with $Q = 2^\mu$ and $S = 2^{\nu-\mu}$ and obtain

$$|S_1|^2 \ll \frac{N^2}{S} + \frac{N}{S}\Re(S_2), \tag{11}$$

with

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

and

$$S_2'(s) = \sum_{n\in I(N,s)} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell (f_{\mu,\lambda}((n+\ell)^2) - f_{\mu,\lambda}((n+\ell+s2^\mu)^2))\right),$$

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

The right hand side of $S_2'(s)$ depends only on the digits of $(n+\ell)^2$ and $(n+\ell+s2^\mu)^2$ between μ and λ. However, we have to take into account also the digits between $\mu' = \mu - \rho'$ and μ, where

$$3 \le \rho' \le \mu/2 \tag{12}$$

will be chosen in a proper way (much smaller than $\mu/2$). We define the integers $u_1 = u_1(n)$, $u_3 = u_3(n)$, $v = v(n)$, $w_1 = w_1(n)$, and $w_3 = w_3(n)$ by the following conditions

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

where U_1, U_3 and V are defined by (3). Then, assuming that

$$\mu \le \nu - \rho' \quad \text{and} \quad 2\mu' \ge \lambda, \tag{13}$$

we observe that (9), (12) and (13) imply the assumptions of Lemma 2 and applying this lemma it follows that

$$\begin{aligned} f_{\mu,\lambda}((n+\ell)^2) &= f_{\rho',\lambda-\mu+\rho'}(u_1 + \ell u_3),\\ f_{\mu,\lambda}((n+\ell+s2^\mu)^2) &= f_{\rho',\lambda-\mu+\rho'}(u_1 + \ell u_3 + v2^{\rho'} + \ell s 2^{\rho'+1}) \end{aligned}$$

for any integer $n < N$ except for at most $O(2^{\nu-\rho'})$ exceptions. Hence it suffices to consider the sum

$$S_3'(s) = \sum_{n\in I(N,s)} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell (f_{\rho',\lambda-\mu+\rho'}(u_1 + \ell u_3) - f_{\rho',\lambda-\mu+\rho'}(u_1 + \ell u_3 + v2^{\rho'} + \ell s 2^{\rho'+1})\right),$$

since we certainly have

$$S_2'(s) = S_3'(s) + O(2^{\nu-\rho'}). \tag{14}$$

Next we rewrite $S_3'(s)$ as

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

where the characteristic functions χ_α are defined by (6). Lemma 11 allows us to replace the product of characteristic functions χ_α by a product of trigonometric polynomials. More precisely, using (51) with $H_1 = U_1 2^{\rho''}$ and $H_3 = U_3 2^{\rho''}$ for some suitable $\rho'' > 0$ (that will be chosen later), we have

$$S_3'(s) = S_4(s) + O(E_1) + O(E_3) + O(E_{1,3}), \tag{15}$$

with, by using the representation of $A_{U_1^{-1},H_1}$ and $A_{U_3^{-1},H_3}$ we obtain

$$\begin{aligned}S_4(s) =&2^{\mu-\lambda}\sum_{|h_1|\le H_1}\sum_{|h_3|\le H_3}\sum_{0\le h<2^{\lambda-\mu}} a_{h_1}(U_1^{-1},H_1)\,a_{h_3}(U_3^{-1},H_3)\\ &\sum_{0\le u_1<U_1}\sum_{0\le u_3<U_3}\sum_{0\le v<V}\mathrm{e}\left(-\frac{h_1u_1}{U_1}-\frac{h_3u_3}{U_3}-\frac{hv}{V}\right)\\ &\mathrm{e}\left(\sum_{\ell=0}^{k-1}\alpha_\ell(f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3)-f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+v2^{\rho'}+\ell s2^{\rho'+1})\right)\\ &\times\sum_n \mathrm{e}\left(\frac{h_1n^2}{2^\lambda}+\frac{h_3n}{2^\nu}+\frac{2hsn}{2^{\lambda-\mu}}\right),\end{aligned}$$

where by (49),

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

where we have *filtered* the correct value of $v=v(n)$. The error terms E_1, E_3, $E_{1,3}$ can be easily estimated, provided that

$$\rho''<\mu'/2\text{ and }\mu'\ll 2^{\nu-\mu'},\tag{16}$$

with the help of Lemma 16:

$$E_1=\frac{1}{2^{\rho''}}\sum_{|h_1|\le 2^{\rho''}}\left|\sum_n \mathrm{e}\left(\frac{h_1n^2}{2^{\mu'}}\right)\right|\ll 2^{\nu-\rho''}+(2^{\nu-\mu'}+\mu')2^{\mu'/2}\frac{1}{2^{\rho''}}\sum_{1\le h_1\le 2^{\rho''}}\sqrt{\gcd(h_1,2^{\mu'})},$$

and

$$\sum_{1\le h_1\le 2^{\rho''}}\sqrt{\gcd(h_1,2^{\mu'})}\le\sum_{\delta\le\rho''}2^{\delta/2}\sum_{\substack{1\le h_1\le 2^{\rho''}\\ 2^\delta\mid h_1}}1\le\sum_{\delta\le\rho''}2^{\delta/2}2^{\rho''-\delta}\ll 2^{\rho''}\tag{17}$$

so that $E_1\ll 2^{\nu-\rho''}$, and similarly using the estimate (53) and Lemma 16:

$$E_3=\frac{1}{2^{\rho''}}\sum_{|h_3|\le 2^{\rho''}}\left|\sum_n \mathrm{e}\left(\frac{h_32n}{2^{\mu'}}\right)\right|\ll 2^{\nu-\rho''}+\rho''2^{\mu'-\rho''}\ll 2^{\nu-\rho''},$$

$$E_{1,3}=\frac{1}{2^{2\rho''}}\sum_{|h_1|\le 2^{\rho''}}\sum_{|h_3|\le 2^{\rho''}}\left|\sum_n \mathrm{e}\left(\frac{h_1n^2}{2^{\mu'}}+\frac{h_32n}{2^{\mu'}}\right)\right|\ll 2^{\nu-\rho''}.$$

Thus the error terms E_1, E_3, and $E_{1,3}$ are negligible (if $\rho''\to\infty$) and so we just have to concentrate on $S_4(s)$.

The first step in the analysis of the main term of $S_4(s)$ is to observe that we only have to take into account the term that corresponds to $h_1=0$. Namely if $h_1\ne 0$ we can estimate the exponential sum in a simple way. By Lemma 16 we have

$$\sum_n \mathrm{e}\left(\frac{h_1n^2}{2^\lambda}+\frac{h_3n}{2^\nu}+\frac{2hsn}{2^{\lambda-\mu}}\right)\ll\left(N2^{-\lambda}+1+\lambda\right)\sqrt{2^\lambda\gcd(h_1,2^\lambda)}\ll\lambda 2^{\lambda/2}\sqrt{\gcd(h_1,2^\lambda)},$$

and similarly to (17)

$$\sum_{1\le h_1\le H_1}\sqrt{\gcd(h_1,2^\lambda)}\ll H_1$$

so that

$$\sum_{0<|h_1|\le H_1}\sum_{|h_3|\le H_3}\sum_{0\le h<2^{\lambda-\mu}}\left|\sum_n \mathrm{e}\left(\frac{h_1n^2}{2^\lambda}+\frac{h_3n}{2^\nu}+\frac{2hsn}{2^{\lambda-\mu}}\right)\right| \ll \lambda H_1H_3 2^{\lambda/2+\lambda-\mu}.$$

We assume that

$$(\nu-\mu)+2(\lambda-\mu)+2(\rho'+\rho'')\le \lambda/4 \tag{18}$$

(which will be justified later) so that

$$S_4(s)=S_5(s)+O(\lambda 2^{3\lambda/4}), \tag{19}$$

where $S_5(s)$ denotes the part of $S_4(s)$ with $h_1=0$. By applying the triangle inequality and by considering the remaining exponential sum we obtain

$$\begin{aligned}|S_5(s)|\le \frac{1}{U_1U_3V}\sum_{|h_3|\le H_3}\sum_{0\le h<2^{\lambda-\mu}}\sum_{0\le u_3<U_3}&\\ \left|\sum_{0\le u_1<U_1}\sum_{0\le v<V}\mathrm{e}\left(\sum_{\ell=0}^{k-1}\alpha_\ell(f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3)-f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+v2^{\rho'}+\ell s2^{\rho'+1}))-\frac{hv}{V}\right)\right|&\\ \times\min\left(N,\left|\sin\left(\pi\left(\frac{h_3}{2^\nu}+\frac{2hs}{2^{\lambda-\mu}}\right)\right)\right|^{-1}\right).&\end{aligned}$$

By setting $u_1=u_1''+2^{\rho'}u_1'$ and $u_3=u_3''+2^{\rho'}u_3'$ (where $0\le u_1'',u_3''<2^{\rho'}$) we get

$$\begin{aligned}f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3)&=f_{\lambda-\mu}(u_1'+\ell u_3'+i_\ell),\\ f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+v2^{\rho'}+\ell s2^{\rho'+1})&=f_{\lambda-\mu}(u_1'+v+\ell(u_3'+2s)+i_\ell)\end{aligned}$$

with $i_\ell=\lfloor (u_1''+\ell u_3'')/2^{\rho'}\rfloor$. As $I=(i_\ell)_{0\le\ell<k}=(\lfloor (u_1''+\ell u_3'')/2^{\rho'}\rfloor)_{0\le\ell<k}$ is contained in $\mathcal{I}_k$, by (3) we have $U_1U_3V=2^{2(\lambda-\mu)+(\nu+1-\mu)+2\rho'}$ and there are $2^{2\rho'}$ pairs (u_1'',u_3'') so that we get

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

By substituting $u_1'+v$ by another variable $\tilde{u}_1'$, by using the definition of $G^I_{\lambda-\mu}(h,d)$ given in (7) and by replacing the maximum by a sum we obtain

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

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

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

Hence by applying Proposition 1 (replacing λ by $\lambda-\mu$, λ' by $\nu-\mu+1$ and using (9)) we get

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

It is now convenient to take also into account the dependency on s and to average according to it. Provided that

$$\nu-\mu'+\rho''+\lambda-\mu \le \nu-2, \tag{20}$$

we have $|h_3|2^{\lambda-\mu}/2^\nu \le 1/2$ and we obtain from (56)

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

Finally we have

$$\sum_{|h_3|\le H_3} \min\left(2^\nu, \left|\sin\left(\pi h_3 2^{-\nu}\right)\right|^{-1}\right) \ll \nu\, 2^\nu$$

and thus we obtain the estimate

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

Putting all these estimates together, from (10), (11), (14), (15), (19) we finally get the upper bound

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

provided that the conditions (9), (13), (16), (18), (20) hold:

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

For example the choice

$$\lambda = \nu + \frac{\nu}{20} \text{ and } \rho' = \rho'' = \frac{\nu}{200}$$

ensures that the above conditions are satisfied for ν large enough.

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

$$S_0 \ll 2^{\nu(1-\eta')} \ll N^{1-\eta'}$$

which is precisely the statement of Theorem 2.

6. The case K odd

In this section we show that when $K = \alpha_0 + \cdots + \alpha_{k-1}$ is odd, Proposition 2 provides an upper bound for the sum

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

Let μ, λ, ρ and ρ_1 be integers satisfying

$$3 \le \rho_1 < \rho,\ 10\rho < \nu < 2^{2\rho},\ \mu = \nu - 2\rho,\ \text{and } \lambda = \nu + 2\rho. \tag{21}$$

to be chosen later (in (36) and (39)). We apply Lemma 12 with $Q=1$ and $R=2^{\rho}$, we sum trivially for $1\le r\le R_1=2^{\rho_1}$ and obtain

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

where

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

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

$$S_1(r)=S_1'(r)+O(2^{\nu-(\lambda-\nu-\rho)}),$$

where

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

which leads to

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

and by the Cauchy-Schwarz inequality to

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

Let $\rho'\in\mathbb{N}$ to be chosen later (in (36)) such that

$$3\le\rho'\le\rho. \tag{22}$$

Applying Lemma 12 with $Q=2^{\mu}$ and

$$S=2^{2\rho'}\le 2^{\nu-\mu}, \tag{23}$$

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

$$f_\lambda((m+s2^{\mu})^2)-f_\lambda(m^2)=f_{\mu,\lambda}((m+s2^{\mu})^2)-f_{\mu,\lambda}(m^2),$$

we get

$$|S_0|^4 \ll 2^{4\nu-2\rho+2\rho_1}+2^{6\nu+2\rho-2\lambda}+\frac{2^{4\nu}}{S}+\frac{2^{3\nu}}{RS}\sum_{R_1<r<R}\sum_{1\le s<S}|S_2(r,s)|, \tag{24}$$

with

$$\begin{aligned}S_2(r,s) \;=\; \sum_{n\in I_2(r,s)}\mathrm{e}\Bigg(&\sum_{\ell=0}^{k-1}\alpha_\ell\big(f_{\mu,\lambda}((n+\ell)^2)-f_{\mu,\lambda}((n+r+\ell)^2)\\ &-f_{\mu,\lambda}((n+s2^{\mu}+\ell)^2)+f_{\mu,\lambda}((n+s2^{\mu}+r+\ell)^2)\big)\Bigg),\end{aligned}$$

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

We can now make a Fourier analysis as in the case where K is even. Let $\mu'=\mu-\rho'>0$. By (21) and (22) the conditions of Lemma 2 are fullfilled. We define 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 $w_3=w_3(n)$ by condition (2).

According to Lemma 2, uniformly for integers $r, s, \ell \geq 1$ such that $r \leq 2^{\mu'}$, $\ell \leq 2^{\mu'-3}$, the number of integers $n < 2^\nu$ for which at least one of the conditions (4) is satisfied is $\ll 2^{\nu-\rho'}$. Filtering by the values of u_1, u_2, u_3, it follows that

$$\begin{aligned} S_2(r,s) \;=\; & \sum_{0\leq u_1<U_1}\sum_{0\leq u_2<U_2}\sum_{0\leq u_3<U_3} \\ & \sum_{n\in I_2(r,s)} \mathrm{e}\biggl(\sum_{\ell=0}^{k-1}\alpha_\ell\bigl(f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3) - f_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3) \\ & \qquad -f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+v(n)2^{\rho'}+\ell s 2^{\rho'+1}) \\ & \qquad +f_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3+v(n)2^{\rho'}+(\ell+r)s2^{\rho'+1})\bigr)\biggr) \\ & \chi_{U_1^{-1}}\left(\frac{n^2}{2^\lambda}-\frac{u_1}{U_1}\right)\chi_{U_2^{-1}}\left(\frac{(n+r)^2}{2^\lambda}-\frac{u_2}{U_2}\right)\chi_{U_3^{-1}}\left(\frac{2n}{2^\nu}-\frac{u_3}{U_3}\right) \\ & +O(2^{\nu-\rho'}), \end{aligned}$$

where U_1, U_2, U_3 and V are defined by (3) and the characteristic functions χ_α are defined by (6). Lemma 11 allows us again to replace the product of characteristic functions χ_α by a product of trigonometric polynomials. More precisely, using (51) with $U_1 = U_2 = U$ and

$$H_1 = H_2 = U\,2^{\rho_2},\ H_3 = U_3\,2^{\rho_3}, \tag{25}$$

where the integers ρ_2 and ρ_3 verify

$$0 < \rho_2 \leq \rho' \quad \text{and} \quad 0 < \rho_3 \leq \rho', \tag{26}$$

we obtain

$$\begin{aligned} S_2(r,s) = S_3(r,s) \;&+\; O(2^{\nu-\rho'}) + O\left(E_3(r)\right) + O\left(E_1\right) + O\left(E_2(r)\right) \\ &+\; O\left(E_{2,3}(0)\right) + O\left(E_{2,3}(r)\right) + O\left(E_{1,2}(r)\right) + O\left(E_{1,2,3}(r)\right), \end{aligned} \tag{27}$$

with

$$\begin{aligned} S_3(r,s) \;=\; & \sum_{0\leq u_1<U}\sum_{0\leq u_2<U}\sum_{0\leq u_3<U_3}\sum_{0\leq v<V} \\ & \mathrm{e}\biggl(\sum_{\ell=0}^{k-1}\alpha_\ell\bigl(f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3) - f_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3) \\ & \qquad -f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+v2^{\rho'}+\ell s 2^{\rho'+1}) \\ & \qquad +f_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3+v2^{\rho'}+(\ell+r)s2^{\rho'+1})\bigr)\biggr) \\ & \sum_{n\in I_2(r,s)} A_{U^{-1},H_1}\left(\frac{n^2}{2^\lambda}-\frac{u_1}{U}\right)A_{U^{-1},H_2}\left(\frac{(n+r)^2}{2^\lambda}-\frac{u_2}{U}\right)A_{U_3^{-1},H_3}\left(\frac{2n}{2^\nu}-\frac{u_3}{U_3}\right) \\ & \frac{1}{2^{\lambda-\mu}}\sum_{0\leq h<2^{\lambda-\mu}}\mathrm{e}\left(h\frac{2sn-v}{2^{\lambda-\mu}}\right). \end{aligned}$$

The sums E_1, $E_2(r)$, $E_3(r)$, $E_{1,2}(r)$, $E_{1,3}$, $E_{2,3}(r)$, $E_{1,2,3}(r)$ can be estimated by elementary exponential sums arguments:

$$E_3(r) = \frac{U_3}{H_3}2^\nu + \frac{U_3}{H_3}\sum_{1\le h_3\le H_3/U_3}\left|\sum_n \mathrm{e}\left(\frac{2h_3U_3n}{2^\nu}\right)\right|$$

gives by (55), (3), (25), (26) and (21), observing that since $\rho_3 \le \rho < \mu - 7\rho < \mu - \rho' - 2$ we sum over less than a period and $\mu < \nu \le 2^{2\rho}$:

$$E_3(r) \ll 2^{\nu-\rho_3} + 2^{-\rho_3}\sum_{1\le h_3\le 2^{\rho_3}}\left|\sin\frac{\pi h_3}{2^{\mu-\rho'-2}}\right|^{-1} \ll 2^{\nu-\rho_3} + \mu\, 2^{\mu-\rho'-\rho_3} \ll 2^{\nu-\rho_3};$$

$$E_2(r) = \frac{U}{H_2}\sum_{|h_2|\le H_2/U}\left|\sum_n \mathrm{e}\left(\frac{h_2(n+r)^2}{2^\lambda/U}\right)\right|$$

gives by (59) (for which we have at most $2^{\nu-\mu+\rho'}$ complete sums), (21), (25) and (26)

$$E_2(r) \ll 2^{\nu-\rho_2} + 2^{-\rho_2}\sum_{1\le h_2\le 2^{\rho_2}}\left(2^{\nu-\mu+\rho'} + \mu - \rho'\right)2^{\frac{\mu-\rho'}{2}}\sqrt{\gcd(h_2, 2^{\mu-\rho'})},$$

hence, since $\mu < \nu \le 2^{2\rho} \le 2^{\nu-\mu+\rho'}$ (by (21)), observing that $\rho_2 \le \rho \le \frac{\mu}{8} \le \frac{1}{2}(\mu-\rho) \le \frac{1}{2}(\mu-\rho')$ (by (21) and (26)), we get similarly to (17),

$$E_2(r) \ll 2^{\nu-\rho_2} + 2^{\nu-\frac{\mu-\rho'}{2}} \ll 2^{\nu-\rho_2};$$

Similarly we have

$$E_1 = \frac{U}{H_1}\sum_{|h_1|\le H_1/U}\left|\sum_n \mathrm{e}\left(\frac{h_1n^2}{2^\lambda/U}\right)\right| \ll 2^{\nu-\rho_2};$$

$$E_{2,3}(r) = \frac{U}{H_2}\frac{U_3}{H_3}\sum_{|h_2|\le H_2/U}\sum_{|h_3|\le H_3/U_3}\left|\sum_n \mathrm{e}\left(\frac{h_2(n+r)^2}{2^\lambda/U} + \frac{2h_3n}{2^\nu/U_3}\right)\right|$$

similarly gives by (59), (17), (21), (25) and (26), with a trivial summation over h_3,

$$E_{2,3}(r) \ll 2^{\nu-\rho_2} + 2^{-\rho_2}\sum_{1\le h_2\le 2^{\rho_2}} 2^{\nu-\mu+\rho'}2^{\frac{\mu-\rho'}{2}}\sqrt{\gcd(h_2, 2^{\mu-\rho'})} \ll 2^{\nu-\rho_2};$$

Similarly we have

$$E_{1,3} = \frac{U}{H_1}\frac{U_3}{H_3}\sum_{|h_1|\le H_1/U}\sum_{|h_3|\le H_3/U_3}\left|\sum_n \mathrm{e}\left(\frac{h_1n^2}{2^\lambda/U} + \frac{2h_3n}{2^\nu/U_3}\right)\right| \ll 2^{\nu-\rho_2};$$

$$E_{1,2}(r) = \frac{U^2}{H_2^2}\sum_{|h_1|\le H_1/U}\sum_{|h_2|\le H_2/U}\left|\sum_n \mathrm{e}\left(\frac{h_1n^2 + h_2(n+r)^2}{2^\lambda/U}\right)\right|$$

similarly gives by (59), (17), (21), (25) and (26), writing $h = h_1 + h_2$,

$$E_{1,2}(r) \ll 2^{\nu-\rho_2} + 2^{-\rho_2}\sum_{1\le h\le 2^{\rho_2+1}} 2^{\nu-\mu+\rho'}2^{\frac{\mu-\rho'}{2}}\sqrt{\gcd(h, 2^{\mu-\rho'})} \ll 2^{\nu-\rho_2}$$

and

$$E_{1,2,3}(r) = \frac{U^2}{H_2^2}\frac{U_3}{H_3}\sum_{|h_1|\le H_1/U}\sum_{|h_2|\le H_2/U}\sum_{|h_3|\le H_3/U_3}\left|\sum_n \mathrm{e}\left(\frac{h_1n^2 + h_2(n+r)^2}{2^\lambda/U} + \frac{2h_3n}{2^\nu/U_3}\right)\right|$$

similarly gives by (59), (17), (21), (25) and (26), writing $h = h_1 + h_2$, with a trivial summation over h_3,

$$E_{1,2,3}(r) \ll 2^{\nu-\rho_2} + 2^{-\rho_2} \sum_{1\le h\le 2^{\rho_2+1}} 2^{\nu-\mu+\rho'} 2^{\frac{\mu-\rho'}{2}} \sqrt{\gcd(h, 2^{\mu-\rho'})} \ll 2^{\nu-\rho_2}.$$

We deduce from (27) that

$$S_2(r,s) = S_3(r,s) + O(2^{\nu-\rho'}) + O(2^{\nu-\rho_2}) + O(2^{\nu-\rho_3}) \tag{28}$$

and we can write

$$\begin{aligned} S_3(r,s) \;=\; & 2^{\mu-\lambda} \sum_{0\le h<2^{\lambda-\mu}} \sum_{|h_1|\le H_1} a_{h_1}(U^{-1}, H_1) \sum_{|h_2|\le H_2} a_{h_2}(U^{-1}, H_2) \sum_{|h_3|\le H_3} a_{h_3}(U_3^{-1}, H_3) \\ & \sum_{0\le u_1<U} \sum_{0\le u_2<U} \sum_{0\le u_3<U_3} \sum_{0\le v<V} \mathrm{e}\left(-\frac{h_1u_1+h_2u_2}{U} - \frac{h_3u_3}{U_3} - \frac{hv}{V}\right) \\ & \mathrm{e}\Bigg(\sum_{\ell=0}^{k-1} \alpha_\ell \big(f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3) - f_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3) \\ & \qquad - f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+v2^{\rho'}+\ell s 2^{\rho'+1}) \\ & \qquad + f_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3+v2^{\rho'}+(\ell+r)s2^{\rho'+1})\big)\Bigg) \\ & \sum_{n\in I_2(r,s)} \mathrm{e}\left(\frac{h_1n^2 + h_2(n+r)^2}{2^\lambda} + \frac{2h_3n}{2^\nu} + \frac{2hsn}{2^{\lambda-\mu}}\right). \end{aligned}$$

Let us introduce the decomposition

$$S_3(r,s) = S_4(r,s) + S_4'(r,s), \tag{29}$$

where $S_4(r,s)$ denotes the contribution of the terms for which $h_1 + h_2 = 0$ while $S_4'(r,s)$ denotes the contribution of the terms for which $h_1 + h_2 \neq 0$. We have by (59)

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

and it remains to consider $S_4(r,s)$. Setting $u_1 = u_1'' + 2^{\rho'}u_1'$, $u_2 = u_2'' + 2^{\rho'}u_2'$ and $u_3 = u_3'' + 2^{\rho'}u_3'$ (where $0 \le u_1'', u_2'', u_3'' < 2^{\rho'}$) we get

$$\begin{aligned} f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3) &= f_{\lambda-\mu}\left(u_1' + \ell u_3' + \left\lfloor (u_1''+\ell u_3'')/2^{\rho'}\right\rfloor\right), \\ f_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3) &= f_{\lambda-\mu}\left(u_2' + \ell u_3' + \left\lfloor (u_2''+\ell u_3'')/2^{\rho'}\right\rfloor\right), \\ f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+v2^{\rho'}+\ell s2^{\rho'+1}) &= f_{\lambda-\mu}\left(u_1' + v + \ell(u_3'+2s) + \left\lfloor (u_1''+\ell u_3'')/2^{\rho'}\right\rfloor\right) \\ f_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3+v2^{\rho'}+(\ell+r)s2^{\rho'+1}) &= f_{\lambda-\mu}\left(u_2' + v + 2sr + \ell(u_3'+2s) + \left\lfloor (u_2''+\ell u_3'')/2^{\rho'}\right\rfloor\right). \end{aligned}$$

Using the periodicity modulo $2^{\lambda-\mu}(= V)$ we replace the variable v by v_1 such that $v_1 \equiv u_1' + v \bmod 2^{\lambda-\mu}$ and we introduce a new variable v_2 such that

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

If we observe that $U/2^{\rho'} = V$ and write $U_3' = U_3/2^{\rho'}$, we obtain

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

Using (7) this gives

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

where, for any $(u,\tilde{u}) \in \mathbb{N}^2$

$$I(u,\tilde{u}) = \left(\left\lfloor \frac{u}{2^{\rho'}}\right\rfloor, \left\lfloor \frac{u+\tilde{u}}{2^{\rho'}}\right\rfloor, \dots, \left\lfloor \frac{u+(k-1)\tilde{u}}{2^{\rho'}}\right\rfloor\right).$$

This leads to

$$\begin{aligned}
S_4(r,s) \;\ll\; & 2^{2\lambda-2\mu} \sum_{0\le u_1'',u_2'',u_3''<2^{\rho'}} \sum_{|h_2|\le H_2} \min(U^{-2},h_2^{-2}) \sum_{|h_3|\le H_3} \min(U_3^{-1},|h_3|^{-1}) \\
& \sum_{0\le h<2^{\lambda-\mu}} \left|\min\left(2^\nu, \left|\sin \pi \frac{h_2r + 2^{\lambda-\nu}h_3 + 2^\mu hs}{2^{\lambda-1}}\right|^{-1}\right)\right| S_5(h,h_2,s,u_1'',u_2'',u_3''),
\end{aligned}$$

where

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

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

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

By periodicity modulo $2^{\lambda-\mu}$ and taking $h''=h'-h$ the first parenthesis is independent of h and we get

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

where

$$S_6(h_2,s,u'',u_3'') = \sum_{0\le u_3'<U_3'}\sum_{0\le h'<2^{\lambda-\mu}} \left|G_{\lambda-\mu}^{I(u'',u_3'')}(h'-h_2,u_3')\right|^2 \left|G_{\lambda-\mu}^{I(u'',u_3'')}(h',u_3'+2s)\right|^2. \tag{30}$$

We obtain

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

Observing that using (26), (22) and (21) we have

$$\left|h_2r+2^{\lambda-\nu}h_3\right|/2^\mu \le (H_2R+2^{\lambda-\nu}H_3)/2^\mu \le 2^{\lambda-2\mu+\rho'+\rho_2+\rho}+2^{\lambda-2\mu+\rho'+\rho_3+1}\le 1/2,$$

we have by (54)

$$\begin{aligned} &\sum_{0\le h<2^{\lambda-\mu}} \left|\min\left(2^\nu, \left|\sin\pi\frac{h_2r+2^{\lambda-\nu}h_3+2^\mu hs}{2^{\lambda-1}}\right|^{-1}\right)\right|\\ &\ll \gcd(s,2^{\lambda-\mu-1})\min\left(2^\nu, \left|\sin\pi\tfrac{h_2r+2^{\lambda-\nu}h_3}{2^{\lambda-1}}\right|^{-1}\right)+(\lambda-\mu)2^{\lambda-\mu} \end{aligned}$$

and by (21) we have $\lambda-\mu=4\rho<\nu$, thus $2^{\lambda-\mu}\ll\min\left(2^{\nu},\left|\sin\pi\frac{h_2r+2^{\lambda-\nu}h_3}{2^{\lambda-1}}\right|^{-1}\right)$, it follows

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

We recall here that in (24) we have $R_1<r<R$ and introduce the integers H_2' and κ such that

$$H_2'=2^{\lambda-\nu+1}H_3/R_1=2^{\lambda-\mu+\rho'+\rho_3-\rho_1+2}=2^{\kappa}. \tag{31}$$

By (3), assuming that

$$\rho'+\rho_3+2<\rho_1, \tag{32}$$

we will have $H_2'<2^{\lambda-\mu}$ and the condition $|h_2|>H_2'$ ensures that $2^{\lambda-\nu}\,|h_3|\le\frac12\,|h_2r|$. 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 respectively the contribution above of the terms $|h_2|\le H_2'$, $H_2'<|h_2|\le 2^{\lambda-\mu}$, $2^{\lambda-\mu}<|h_2|\le H_2$.

6.1. **Estimate of** $S_{41}(r,s)$**.** By (25), (26), (3) and by (21) we have $H_3=2^{\nu-\mu+\rho'+\rho_3+1}\le 2^{4\rho+1}\le 2^{\nu}$ and by (54) we get

$$\sum_{|h_3|\le H_3}\min\left(2^{\nu},\left|\sin\pi\tfrac{h_3+h_2r2^{\nu-\lambda}}{2^{\nu-1}}\right|^{-1}\right)\ll\nu 2^{\nu},$$

so that

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

By Proposition 2 (replacing λ by $\lambda-\mu$ and L by $\lambda-\mu-\kappa$), we have for some $0<\eta\le 1$

$$\left|G_{\lambda-\mu}^{I(u'',u_3'')}(h'-h_2,u_3')\right|\ll 2^{-\eta(\lambda-\mu-\kappa)}\max_{J\in\mathcal{I}_k}\left|G_{\kappa}^{J}(h'-h_2,\lfloor u_3'/2^L\rfloor)\right|.$$

By Parseval's equality and recalling that $\operatorname{card}\mathcal{I}_k=2^{k-1}$ it follows that

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

We obtain uniformly in λ, μ, H_2', u_3', u'' and u_3'':

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

Hence it follows from (30) and Parseval's equality that

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

and by the Cauchy-Schwarz inequality we obtain

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

This gives

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

so that by (31), (3) and (57)

$$\frac{1}{RS}\sum_{R_1<r<R}\sum_{1\le s<S} S_{41}(r,s) \ll \nu\,(\lambda-\mu)^2\ 2^{\nu-\eta(\rho_1-\rho'-\rho_3)}. \tag{33}$$

6.2. **Estimate of $S_{42}(r,s)$.** The condition $|h_2|>H_2'$ ensures that $2^{\lambda-\nu}|h_3|\le \frac12|h_2 r|$ so that

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

By the Cauchy-Schwarz inequality we have

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

It follows that

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

and recalling that $U_3' = U_3/2^{\rho'}$ we get by (31) and (3),

$$S_{42}(r,s) \ll (\lambda-\mu)^2\ \frac{\gcd(s,2^{\lambda-\mu-1})}{r} 2^{\nu+\rho_1-\rho_3},$$

so that by (57)

$$\frac{1}{RS}\sum_{R_1<r<R}\sum_{1\le s<S} S_{42}(r,s) \ll \rho\ (\lambda-\mu)^3\ 2^{\nu-\rho+\rho_1-\rho_3}. \tag{34}$$

6.3. **Estimate of $S_{43}(r,s)$.** We will split the summation over h_2 into $J = H_2/2^{\lambda-\mu}-1$ parts of the form $j2^{\lambda-\mu}<|h_2|\le (j+1)2^{\lambda-\mu}$ with $j=1,\dots,J$. The condition $|h_2|>j2^{\lambda-\mu}$ implies that

$$2^{2\lambda-2\mu}\min(U^{-2}, h_2^{-2}) < j^{-2}$$

and ensures that $2^{\lambda-\nu}|h_3|\le \frac12|h_2 r|$ so that

$$\min\left(2^{\nu}, \left|\sin \pi \tfrac{h_2 r + 2^{\lambda-\nu}h_3}{2^{\lambda-1}}\right|^{-1}\right) \ll \frac{2^{\lambda}}{j2^{\lambda-\mu} r} = \frac{2^{\mu}}{jr}.$$

By the Cauchy-Schwarz inequality we have

$$\sum_{j2^{\lambda-\mu}<|h_2|\le(j+1)2^{\lambda-\mu}} S_6(h_2,s,u_1'',u_3'')^{1/2} S_6(h_2,s,u_2'',u_3'')^{1/2}$$
$$\ll \Big(\sum_{h_2 \bmod 2^{\lambda-\mu}} S_6(h_2,s,u_1'',u_3'')\Big)^{1/2}\Big(\sum_{h_2 \bmod 2^{\lambda-\mu}} S_6(h_2,s,u_2'',u_3'')\Big)^{1/2} \ll U_3'.$$

It follows that

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

so that by (3) and (57)

$$\frac{1}{RS}\sum_{R_1<r<R}\sum_{1\le s<S} S_{43}(r,s) \ll \rho\ (\lambda-\mu)^3\ 2^{\nu-\rho+3\rho'}. \tag{35}$$

It follows from (33), (34) and (35) that

$$\frac{1}{RS}\sum_{R_1<r<R}\sum_{1\le s<S}|S_4(r,s)| \ll \nu^4 2^\nu\left(2^{-\eta(\rho_1-\rho'-\rho_3)}+2^{-\rho+\rho_1-\rho_3}+2^{-\rho+3\rho'}\right).$$

Choosing

$$\rho = 4\rho',\ \rho_1 = 3\rho',\ \rho_2=\rho_3=\rho', \tag{36}$$

using (22) we see that condition (32) is satisfied and we obtain (since $0<\eta<1$)

$$\frac{1}{RS}\sum_{R_1<r<R}\sum_{1\le s<S}|S_4(r,s)| \ll \nu^4 2^\nu\left(2^{-\eta\rho'}+2^{-2\rho'}+2^{-\rho'}\right) \ll \nu^4 2^{\nu-\eta\rho'}. \tag{37}$$

Using (29) and (28), we obtain

$$\frac{1}{RS}\sum_{R_1<r<R}\sum_{1\le s<S}|S_2(r,s)| \ll \nu^4 2^\nu\left(2^{-\eta\rho'}+2^{\frac12(8\lambda-9\mu+8\rho')}\right) \tag{38}$$

that we can insert in (24), recalling by (23) that $S=2^{2\rho'}$ and by (21) that $\mu=\nu-2\rho$, $\lambda=\nu+2\rho$, so that we get

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

Choosing

$$\rho' = \lfloor \nu/146 \rfloor \tag{39}$$

we have $-\frac{\nu}{2}+17\rho+4\rho' \le -73\rho'+68\rho'+4\rho' = -\rho'$ and to check that the condition (21) is satisfied it is enough to observe that $10\rho = 40\rho' < \nu$. We obtain

$$|S_0| \ll \nu 2^{\nu-\frac{\eta\rho'}{4}} \ll \nu N^{1-\eta'} \tag{40}$$

which completes the proof that when K is odd Proposition 2 implies Theorem 2.

7. Proof of Proposition 1

7.1. **Proof of Proposition 1 in the case** $(\alpha_0,\dots,\alpha_{k-1})=(1,\dots,1)$**.** With the help of Lemma 3 it is easy to establish a set of recurrences for

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

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

$$\begin{aligned}\Phi_{\lambda,\lambda'}^{I,I'}(h)&=\frac{(-1)^{|I|+|I'|}}{8}\\&\times\Big(\Phi_{\lambda-1,\lambda'-1}^{T_{00}(I),T_{00}(I')}(h)+\mathrm{e}(h/2^\lambda)\Phi_{\lambda-1,\lambda'-1}^{T_{00}(I),T_{01}(I')}(h)+\mathrm{e}(-h/2^\lambda)\Phi_{\lambda-1,\lambda'-1}^{T_{01}(I),T_{00}(I')}(h)+\Phi_{\lambda-1,\lambda'-1}^{T_{01}(I),T_{01}(I')}(h)\\&\quad+\Phi_{\lambda-1,\lambda'-1}^{T_{10}(I),T_{10}(I')}(h)+\mathrm{e}(h/2^\lambda)\Phi_{\lambda-1,\lambda'-1}^{T_{10}(I),T_{11}(I')}(h)+\mathrm{e}(-h/2^\lambda)\Phi_{\lambda-1,\lambda'-1}^{T_{11}(I),T_{10}(I')}(h)+\Phi_{\lambda-1,\lambda'-1}^{T_{11}(I),T_{11}(I')}(h)\Big).\end{aligned}$$

This gives rise to a vector recurrence for $\boldsymbol{\psi}_{\lambda,\lambda'}(h)=\Big(\Phi_{\lambda,\lambda'}^{I,I'}(h)\Big)_{(I,I')\in\mathcal{I}_k^2}$ of the form

$$\boldsymbol{\psi}_{\lambda,\lambda'}(h)=\mathbf{M}(h/2^\lambda)\cdot\boldsymbol{\psi}_{\lambda-1,\lambda'-1}(h),$$

where the $2^{2(k-1)}\times 2^{2(k-1)}$-matrix $\mathbf{M}(\beta)=(M_{(I,I'),(J,J')}(\beta)))_{((I,I'),(J,J'))\in\mathcal{I}_k^2\times\mathcal{I}_k^2}$ is independent of λ and λ' (we put $\beta=h/2^\lambda$). By construction all absolute row sums of $\mathbf{M}(\beta)$ can be estimated to be ≤ 1. More precisely in each row there are (in total) eight non-zero terms, where all of them are either equal to $\pm 1/8$ or equal to $\pm\,\mathrm{e}(\pm\beta)/8$. Note that it might occur that, for example, $(T_{00}(I),T_{00}(I'))=(T_{00}(I),T_{01}(I'))$ for some (I,I') so that some entries of the matrix $\mathbf{M}(\beta)$ consists of a sum of several term of the form $\pm 1/8$ or $\pm\,\mathrm{e}(\pm\beta)/8$. For example, if $k=4$ and $I=I'=(0,0,0,0)$ then we have (with $J_1=(0,0,1,1)$ and $J_2=(0,1,1,2)$)

$$\begin{aligned}\Phi_{\lambda,\lambda'}^{\mathbf{0},\mathbf{0}}(h)=\frac{1}{8}\Big(&\big(2+\mathrm{e}(h/2^\lambda)+\mathrm{e}(-h/2^\lambda)\big)\,\Phi_{\lambda-1,\lambda'-1}^{\mathbf{0},\mathbf{0}}(h)+\Phi_{\lambda-1,\lambda'-1}^{J_1,J_1}(h)+\\&+\mathrm{e}(h/2^\lambda)\Phi_{\lambda-1,\lambda'-1}^{J_1,J_2}(h)+\mathrm{e}(-h/2^\lambda)\Phi_{\lambda-1,\lambda'-1}^{J_2,J_1}(h)+\Phi_{\lambda-1,\lambda'-1}^{J_2,J_2}(h)\Big)\end{aligned}$$

so that the first row of the matrix has just 5 non-zero entries and the first entry comprises 4 terms.

It is convenient to interpret these matrices as weighted directed multi-graphs, where the vertices are the pairs $(I,I')\in\mathcal{I}_k^2$ and starting from each vertex there are eight directed edges to the vertices $(T_{\varepsilon\varepsilon'}(I),T_{\varepsilon\varepsilon''}(I'))$ (where $(\varepsilon,\varepsilon',\varepsilon'')\in\{0,1\}^3$) with the corresponding weights $1/8$ or $\mathrm{e}(\pm\beta)/8$ (with the common sign $(-1)^{|I|+|I'|}$), see Figure 1. Note again that different edges might connect the same pair of vertices so that we get multiple edges (and even multiple loops). Of course products of

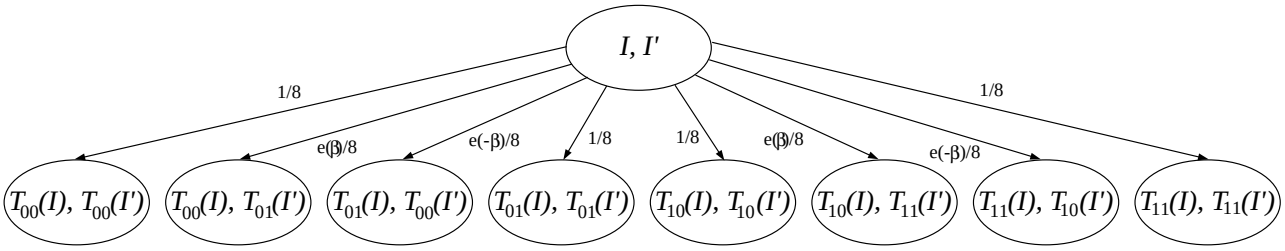


Figure 1. Weighted directed graph representation of the recurrence for $\Phi_{\lambda,\lambda'}^{I,I'}(h)$ (the common sign of all the edge weights is $(-1)^{|I|+|I'|}$).

m such matrices correspond to oriented paths of length m on these graphs, where such paths are

weighted with the corresponding products (of modulus 8^{-m}). The entries at position $((I,I'),(J,J'))$ of such product matrices correspond then to the sum of weights of paths from (I,I') to (J,J').

In order to prove Proposition 1 it is enough to check the conditions of Lemma 17 uniformly in h for $\mathbf{M}_\ell = \mathbf{M}(h/2^\ell)$. Indeed, as for $\frac{1}{2}\lambda \le \lambda' \le \lambda$ we have

$$\boldsymbol{\psi}_{\lambda,\lambda'}(h) = \mathbf{M}(h/2^\lambda)\cdots\mathbf{M}(h/2^{\lambda-\lambda'+1})\boldsymbol{\psi}_{\lambda-\lambda',0}(h),$$

it follows by applying (60) with $k=\lambda'$ and $r=\lambda-\lambda'+1$ that

$$\|\boldsymbol{\psi}_{\lambda,\lambda'}(h)\|_\infty \le C2^{-\delta\lambda'}\,\|\boldsymbol{\psi}_{\lambda-\lambda',0}(h)\|_\infty \le C2^{-\delta\lambda'} \ll 2^{-\delta\lambda/2} \tag{41}$$

and consequently

$$\Phi^{I,I}_{\lambda,\lambda'}(h) = \frac{1}{2^{\lambda'}}\sum_{0\le d<2^{\lambda'}} \left|G^I_\lambda(h,d)\right|^2 \le \|\boldsymbol{\psi}_{\lambda,\lambda'}(h)\|_\infty \ll 2^{-\delta\lambda/2}.$$

We first show that there exists an integer $m_0 \ge 1$ such that every product

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

of m_0 consecutive matrices $\mathbf{M}_\ell = \mathbf{M}(h/2^\ell)$ verifies the condition (1) of Lemma 17. It is clear that $T_{00}^m(I) = \mathbf{0}$ for all $I\in\mathcal{I}_k$ if m is sufficiently large, which means in the graph interpretation (see Figure 1) that for every vertex (I,I') there is a path of length m from (I,I') to $(\mathbf{0},\mathbf{0})$. Let m_0 be one of these values and fix a row indexed by (I,I') in the matrix $\mathbf{A}$. From the graph interpretation it is clear that the entry $A_{(I,I'),(\mathbf{0},\mathbf{0})}$ is the sum of at least one term of modulus 8^{-m_0}. Now there are two possible cases. If the absolute row sum is $\le 1-8^{-m_0}/2$ then we are done. However, if the absolute row sum is $> 1-8^{-m_0}/2$ then it follows that $|A_{(I,I'),(\mathbf{0},\mathbf{0})}| \ge 8^{-m_0}/2$. Indeed the inequality $|A_{(I,I'),(\mathbf{0},\mathbf{0})}| < 8^{-m_0}/2$ would imply that $A_{(I,I'),(\mathbf{0},\mathbf{0})}$ is the sum of at least two terms of modulus 8^{-m_0}, so that the absolute row sum would be bounded by

$$\sum_{(J,J')} |A_{(I,I'),(J,J')}| < \frac{1}{2}8^{-m_0} + \left(1-2\cdot 8^{-m_0}\right) = 1-\frac{3}{2}8^{-m_0},$$

which would contradict the assumption that the absolute row sum is $> 1-8^{-m_0}/2$. This shows that condition (1) of Lemma 17 is satisfied with $c_0 = \eta = \frac{1}{2}8^{-m_0}$.

Finally we show that there exists an integer $m_1 \ge 1$ such that every product

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

of m_1 consecutive matrices $\mathbf{M}_\ell = \mathbf{M}(h/2^\ell)$ verifies the condition (2) of Lemma 17. Indeed we will concentrate on the entry $B_{(\mathbf{0},\mathbf{0}),(\mathbf{0},\mathbf{0})}$, that is, we will 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 is due to the structure of this entry. Since $T_{00}(\mathbf{0}) = T_{01}(\mathbf{0}) = \mathbf{0}$ 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 modulus 8^{-m_1} (for every $m_1 \ge 1$), that is, 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. For $m_1 \ge 3$, starting from $(\mathbf{0},\mathbf{0})$ we first apply m_1-2 times the transformations (T_{00},T_{00}), then one time the transformation (T_{00},T_{01}), and then one time the transformation (T_{00},T_{00}). This corresponds in the graph interpretation (see Figure 1) to a path from $(\mathbf{0},\mathbf{0})$ to $(\mathbf{0},\mathbf{0})$ of length m_1 with weight $\mathrm{e}(h/2^{\lambda-m_1+1})8^{-m_1}$.

Next we observe that $T_{11}(\mathbf{0})$ has $k-1$ non-zero entries and we recall that $k-1$ is odd. Thus, there exists $m_1 \ge 4$ such that $T_{01}^{m_1-3}T_{11}(\mathbf{0})$ is of the form $011\cdots1$, that is, it has an odd number of 1's. Starting from $(\mathbf{0},\mathbf{0})$ we apply now one time the transformation (T_{11},T_{11}), then m_1-3 times the transformation (T_{01},T_{01}), then one time the transformations (T_{00},T_{01}), and then one time the transformation (T_{00},T_{00}). This corresponds in the graph interpretation (see Figure 1) to a path from $(\mathbf{0},\mathbf{0})$ to $(\mathbf{0},\mathbf{0})$ of length m_1 with weight $(-1)^{|\mathbf{0}|+|(0,1,\ldots,1)|}\,\mathrm{e}(h/2^{\lambda-m_1+1})8^{-m_1} = -\,\mathrm{e}(h/2^{\lambda-m_1+1})8^{-m_1}$.

Thus we have shown that at least two terms cancel for a properly chosen m_1. Of course this implies

$$|B_{(\mathbf{0},\mathbf{0}),(\mathbf{0},\mathbf{0})}| \le (k_0-2)8^{-m_1},$$

so that

$$\sum_{(J,J')} |B_{(0,0),(J,J')}| \le (k_0-2)8^{-m_1} + (1-k_0 8^{-m_1}) \le 1 - 2\cdot 8^{-m_1},$$

so that condition (2) of Lemma 17 is verified with $\eta = 2\cdot 8^{-m_1}$, which completes the proof of Proposition 1 when $(\alpha_0,\dots,\alpha_{k-1}) = (1,\dots,1)$ and K is even.

7.2. **Proof of Proposition 1 in the case** $(\alpha_0,\dots,\alpha_{k-1}) \ne (1,\dots,1)$**.** Without loss of generality we can assume that $\alpha_0 = 1$ and that for at least one $\ell \ge 1$ we have $\alpha_\ell = 0$. As the discrete Fourier transform G_λ^I only depends on those indices ℓ for which $\alpha_\ell = 1$, let us introduce the reduced K-uple $\tilde I = (i_\ell)_{0\le \ell<k,\, \alpha_\ell=1}$ and the reduced sets $\tilde{\mathcal{I}}_k = \{\tilde I,\ I\in\mathcal{I}_k\}$.

Then the proof of Proposition 1 works in the case $(\alpha_0,\dots,\alpha_{k-1}) \ne (1,\dots,1)$ in the same way as in the case $(\alpha_0,\dots,\alpha_{k-1}) = (1,\dots,1)$ if we replace $\mathcal{I}_k$ by $\tilde{\mathcal{I}}_k$, G_λ^I by $G_\lambda^{\tilde I}$ and for any $(\varepsilon,\varepsilon')\in\{0,1\}^2$ the transformation $T_{\varepsilon\varepsilon'}$ on $\mathcal{I}_k$ by the corresponding transformation $\tilde T_{\varepsilon\varepsilon'}$ on $\tilde{\mathcal{I}}_k$. In particular, working with

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

instead of $\Phi_{\lambda,\lambda'}^{I,I'}(h)$, the corresponding recurrence is exactly the same. Furthermore the matrices $\mathbf{M}(\beta)$ have now dimension $|\tilde{\mathcal{I}}_k|^2\times|\tilde{\mathcal{I}}_k|^2$ instead of $2^{2(k-1)}\times 2^{2(k-1)}$ and, of course, the corresponding weighted directed graph has less vertices. If we replace k by K (and use the fact that K is even) then we prove in the same way like in Section 7.1 that the conditions of Lemma 17 are satisfied.

This completes the proof of Proposition 1 in the case where K is even.

8. Proof of Proposition 2

8.1. **Proof of Proposition 2 in the case** $(\alpha_0,\dots,\alpha_{k-1}) = (1,\dots 1)$**.** Formula (8) can be written as

$$\mathbf{G}_\lambda(h,d) = \frac{1}{2}\mathbf{M}^{\varepsilon_0(d)}\left(\mathrm{e}(-h/2^\lambda)\right)\mathbf{G}_{\lambda-1}(h,\lfloor d/2\rfloor),$$

with for any $\varepsilon\in\{0,1\}$ and $z\in\mathbb{U}$,

$$\mathbf{M}^\varepsilon(z) = \left(\mathbb{1}_{[J=T_{\varepsilon 0}(I)]}w_{\varepsilon 0}(I,z) + \mathbb{1}_{[J=T_{\varepsilon 1}(I)]}w_{\varepsilon 1}(I,z)\right)_{(I,J)\in\mathcal{I}_k^2},$$

where for any $\varepsilon'\in\{0,1\}$,

$$w_{\varepsilon\varepsilon'}(I,z) = (-1)^{|I|+\varepsilon\sigma+\varepsilon' K}z^{\varepsilon'} = (-1)^{|I|+\varepsilon\sigma+\varepsilon'}z^{\varepsilon'}$$

(as $K=k$ is odd) and $\mathbb{1}_{[\mathcal{P}]}=1$ if the proposition $\mathcal{P}$ is true and $\mathbb{1}_{[\mathcal{P}]}=0$ otherwise. It follows by induction that for any integer $n\ge 1$, we have

$$\mathbf{G}_\lambda(h,d) = \frac{1}{2^m}\mathbf{M}^{\varepsilon_0(d)\dots\varepsilon_{m-1}(d)}\left(\mathrm{e}(-h/2^\lambda)\right)\mathbf{G}_{\lambda-m}(h,\lfloor d/2^m\rfloor),$$

where for any $\mathbf{d}=(d_0,\dots,d_{m-1})\in\{0,1\}^m$ we put

$$\mathbf{M}^{\mathbf{d}}(z) = \mathbf{M}^{d_0\dots d_{m-1}}(z) = \mathbf{M}^{d_0}(z)\cdots\mathbf{M}^{d_{m-1}}(z^{2^{m-1}})$$

and we define the polynomials $P_{IJ}^{\mathbf{d}}$ for $(I,J)\in\mathcal{I}_k^2$ by

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

so that

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

$\|\mathbf{A}\|_\infty$ denotes the matrix row-sum norm of $\mathbf{A}$ (see Section 9.5). Proposition 2 will follow from the fact that there exists an integer $m \geq 1$ (which will be actually $k+1$) such that for any $\mathbf{d} \in \{0,1\}^m$, $I \in \mathcal{I}_k$, and $z \in \mathbb{U}$

$$\sum_{J\in\mathcal{I}_k} \left|P^{\mathbf{d}}_{IJ}(z)\right| < 2^m. \tag{42}$$

For this purpose we can apply Lemma 17 with matrices $\frac{1}{2}\mathbf{M}^{\varepsilon_0(d)}\left(\mathrm{e}(-h/2^\lambda)\right)$, with $m_0 = m_1 = m$, and

$$\eta = 1 - \frac{1}{2^m} \max_{\mathbf{d}\in\{0,1\}^m} \max_{I\in\mathcal{I}_k} \max_{z\in\mathbb{U}} \sum_{J\in\mathcal{I}_k} \left|P^{\mathbf{d}}_{IJ}(z)\right| > 0$$

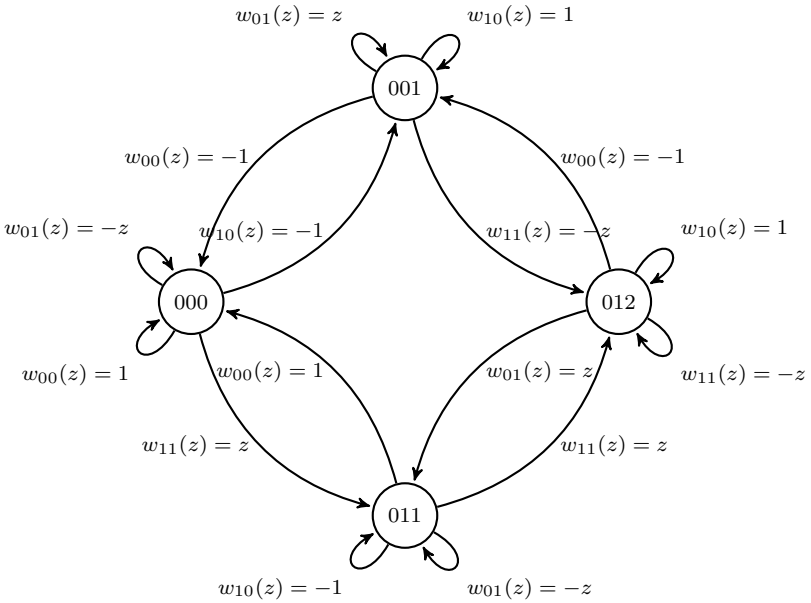
(we do not need c_0 since all absolute row sums are $\leq 1-\lambda$). The rest of this section is devoted to a proof of (42).

Let $\mathcal{G}(z)$ be the weighted directed multi-graph of outdegree 4 whose vertices are the elements of $\mathcal{I}_k$ and where for each $(\varepsilon,\varepsilon') \in \{0,1\}^2$ and $I \in \mathcal{I}_k$ the edge from I to $T_{\varepsilon\varepsilon'}(I)$ has weight $w_{\varepsilon\varepsilon'}(I,z)$.

For example when $k=3$ we have

$$\mathbf{M}^0(z) = \begin{pmatrix} 1-z & 0 & 0 & 0 \\ -1 & z & 0 & 0 \\ 1 & 0 & -z & 0 \\ 0 & -1 & z & 0 \end{pmatrix}, \quad \mathbf{M}^1(z) = \begin{pmatrix} 0 & -1 & z & 0 \\ 0 & 1 & 0 & -z \\ 0 & 0 & -1 & z \\ 0 & 0 & 0 & 1-z \end{pmatrix}$$

and $\mathcal{G}(z)$ is the following weighted directed graph:



For any $\mathbf{d} = (d_0,\ldots,d_{m-1}) \in \{0,1\}^m$ we can interpret the coefficients of the matrix $\mathbf{M}^{\mathbf{d}}(z)$ as coding of paths of length m with, for $j \in \{0,\ldots,m-1\}$, step j in the graph $\mathcal{G}(z^{2^j})$. More precisely, for any $I \in \mathcal{I}_k$, $\mathbf{e} = (e_0,\ldots,e_{m-1}) \in \{0,1\}^m$ and $i \in \{1,\ldots,m\}$, let us denote $T^{\mathbf{de}}_i(I) = T_{d_{i-1}e_{i-1}} \circ \cdots \circ T_{d_0e_0}(I)$ and associate to each of the 2^m paths from the vertex I to the vertices $T^{\mathbf{de}}_m(I)$

the weight

$$\begin{aligned} w^{\mathbf{de}}(I,z) &= w_{d_0e_0}(I,z)w_{d_1e_1}(T_1^{\mathbf{de}}(I),z^2)\cdots w_{d_{m-1}e_{m-1}}(T_{m-1}^{\mathbf{de}}(I),z^{2^{m-1}}) \\ &= (-1)^{\nu(I,\mathbf{d},\mathbf{e})}z^{N(\mathbf{e})}, \end{aligned}$$

with

$$\nu(I,\mathbf{d},\mathbf{e}) = |I| + \left|T_1^{\mathbf{de}}(I)\right| + \cdots + \left|T_{m-1}^{\mathbf{de}}(I)\right| + |\mathbf{d}|\,\sigma + |\mathbf{e}| \tag{43}$$

and

$$N(\mathbf{e}) = \sum_{i=0}^{m-1} e_i 2^i, \tag{44}$$

where $|\mathbf{d}| = \sum_{i=0}^{m-1}|d_i|$. Then, for any $(I,J)\in\mathcal{I}_k^2$, we have, by definition of $P_{IJ}^{\mathbf{d}}$:

$$P_{IJ}^{\mathbf{d}}(z) = \sum_{\substack{\mathbf{e}\in\{0,1\}^m \\ T_m^{\mathbf{de}}(I)=J}} w^{\mathbf{de}}(I,z) = \sum_{\substack{\mathbf{e}\in\{0,1\}^m \\ T_m^{\mathbf{de}}(I)=J}} (-1)^{\nu(I,\mathbf{d},\mathbf{e})}z^{N(\mathbf{e})}. \tag{45}$$

Lemma 4. *For any $\mathbf{d}\in\{0,1\}^m$, the family of polynomials $(P_{IJ}^{\mathbf{d}})_{(I,J)\in\mathcal{I}_k^2}$ has the following properties:*

1. *for any $(I,J)\in\mathcal{I}_k^2$, the coefficients of $P_{IJ}^{\mathbf{d}}$ are 0, $+1$ or -1;*
2. *for any $I\in\mathcal{I}_k$ and $j\in\{0,\dots,2^m-1\}$, z^j or $-z^j$ appears exactly once as a monomial of some polynomial $P_{IJ}^{\mathbf{d}}$ ($J\in\mathcal{I}_k$);*
3. *for any $I\in\mathcal{I}_k$,*

$$\begin{aligned} &\operatorname{card}\{j,\ 0\le j<2^m,\ \exists J\in\mathcal{I}_k,\ z^j \text{ appears as a monomial of } P_{IJ}^{\mathbf{d}}\} \\ =&\operatorname{card}\{j,\ 0\le j<2^m,\ \exists J\in\mathcal{I}_k,\ -z^j \text{ appears as a monomial of } P_{IJ}^{\mathbf{d}}\} = 2^{m-1}. \end{aligned}$$

Proof. It follows from (45) that (1) is a direct consequence of the fact that the function N defined by (44) is a bijection between $\{0,1\}^m$ and $\{0,\dots,2^{m-1}\}$ and (2) of the fact that for any $I\in\mathcal{I}_k$, the sets $E(J)=\{\mathbf{e}\in\{0,1\}^m,\ T_m^{\mathbf{de}}(I)=J\}$ form a partition of $\{0,1\}^m$. Moreover, as for any $\varepsilon\in\{0,1\}$ the sum of the coefficients of each line of the matrix $\mathbf{M}^{\varepsilon}(1)$ is equal to zero, it follows that for any $\mathbf{d}\in\{0,1\}^m$ the sum of the coefficients of each line of the matrix $\mathbf{M}^{\mathbf{d}}(1)$ is equal to zero, which proves (3). □

For any $I=(i_0,\dots,i_{k-1})\in\mathcal{I}_k$ we denote $I_{|j}=i_j$.

Lemma 5. *Let $(I_0,I_1)\in\mathcal{I}_k^2$ and $j\in\{0,\dots,k-1\}$ such that $I_{0|j}-I_{1|j}=1$. Then, for any $\varepsilon\in\{0,1\}$, we have either*

$$T_{\varepsilon 0}(I_0)_{|j} = T_{\varepsilon 0}(I_1)_{|j} \quad \text{and} \quad T_{\varepsilon 1}(I_0)_{|j} = T_{\varepsilon 1}(I_1)_{|j}+1$$

or

$$T_{\varepsilon 0}(I_0)_{|j} = T_{\varepsilon 0}(I_1)_{|j}+1 \quad \text{and} \quad T_{\varepsilon 1}(I_0)_{|j} = T_{\varepsilon 1}(I_1)_{|j}.$$

Proof. For $I\in\mathcal{I}_k$, $j\in\{0,\dots,k-1\}$ and $(\varepsilon,\varepsilon')\in\{0,1\}^2$ we have $T_{\varepsilon\varepsilon'}(I)_{|j} = \left\lfloor \frac{I_{|j}+j\varepsilon+\varepsilon'}{2}\right\rfloor$, so that Lemma 5 follows from the fact that for any $(i,i')\in\mathbb{N}^2$ we have either

$$\left\lfloor\frac{i+i'}{2}\right\rfloor = \left\lfloor\frac{i+1+i'}{2}\right\rfloor \quad \text{or} \quad \left\lfloor\frac{i+i'+1}{2}\right\rfloor = \left\lfloor\frac{i+1+i'+1}{2}\right\rfloor.$$

□

Lemma 6. *For any $(d_i)_{i\in\mathbb{N}}\in\{0,1\}^{\mathbb{N}}$ and any $I\in\mathcal{I}_k$ there exist $J=J(I)\in\mathcal{I}_k$, $m=m(I)\in\{1,\dots,k\}$ and $(\mathbf{e},\mathbf{e}')\in\{0,1\}^m\times\{0,1\}^m$, $\mathbf{e}\ne\mathbf{e}'$ such that $J=T_m^{\mathbf{de}}(I)=T_m^{\mathbf{de}'}(I)$ and $N(\mathbf{e}')=N(\mathbf{e})+1$, where $\mathbf{d}=(d_0,\dots,d_{m-1})$.*

Proof. For any $I \in \mathcal{I}_k$ and $e_0 \in \{0,1\}$ we define $I_{e_0} = T_{d_0 e_0}(I)$.

If $d_0 = 0$ and $I = (0,\dots,0)$ or $d_0 = 1$ and $I = (0,1,\dots,k-1)$, we have $I_0 = I_1 = I$ so that Lemma 6 is true in these two cases with $m = 1$.

In any other case, we have $I_0 \neq I_1$ and it remains to find an integer $m \in \{2\dots,k\}$ and $(e_1,\dots,e_{m-1}) \in \{0,1\}^{m-1}$ such that

$$T_{d_{m-1}e_{m-1}} \circ \cdots \circ T_{d_1 e_1}(I_0) = T_{d_{m-1}e_{m-1}} \circ \cdots \circ T_{d_1 e_1}(I_1).$$

Let j_1 be the smallest integer j such that $I_{0|j} = I_{1|j} + 1$ and choose, by Lemma 5, $e_1 \in \{0,1\}$ such that $T_{d_1 e_1}(I_0)_{|j_1} = T_{d_1 e_1}(I_1)_{|j_1} + 0$. By repeating this procedure $m-1 \leq k-1$ times (by construction, for any $i \in \{1,\dots,m\}$ the entries of $T_{d_{i-1}e_{i-1}} \circ \cdots \circ T_{d_0 0}(I)$ and $T_{d_{i-1}e_{i-1}} \circ \cdots \circ T_{d_0 1}(I)$ are equal or differ by 1) and taking $\mathbf{e} = (0, e_1, \dots, e_{m-1})$ and $\mathbf{e}' = (1, e_1, \dots, e_{m-1})$ we obtain Lemma 6. □

Lemma 6 remains valid if for any $I \in \mathcal{I}_k$ we replace $m = m(I)$ by $m = k$ (or any value greater than k) and it shows that for any $m \geq k$, $\mathbf{d} \in \{0,1\}^m$ and $I \in \mathcal{I}_k$ there exist $J \in \mathcal{I}_k$ such that the polynomial $P_{IJ}^{\mathbf{d}}$ contains two monomials of consecutive degrees: $\pm z^{N(\mathbf{e})}$ and $\pm z^{N(\mathbf{e})+1}$. In the next Lemma 7 we make this even more precise by showing that we can find two such monomials of consecutive degrees with different signs: $\nu(I,\mathbf{d},\mathbf{e}) \equiv \nu(I,\mathbf{d},\mathbf{e}') + 1 \bmod 2$.

Lemma 7. *For any $\mathbf{d} \in \{0,1\}^k$ and any $I \in \mathcal{I}_k$ there exist $J \in \mathcal{I}_k$ and $(\mathbf{e},\mathbf{e}') \in \{0,1\}^k \times \{0,1\}^k$, $\mathbf{e} \neq \mathbf{e}'$ such that $J = T_k^{\mathbf{de}}(I) = T_k^{\mathbf{de}'}(I)$, $N(\mathbf{e}') = N(\mathbf{e}) + 1$ and $\nu(I,\mathbf{d},\mathbf{e}') \equiv \nu(I,\mathbf{d},\mathbf{e}) + 1 \bmod 2$.*

Proof. Let us consider for any $\ell \in \{1,\dots,k\}$ the k-tuples $I_0(\ell) = T_{d_{\ell-1}e_{\ell-1}} \circ \cdots \circ T_{d_1 e_1}(I_0)$ and $I_1(\ell) = T_{d_{\ell-1}e_{\ell-1}} \circ \cdots \circ T_{d_1 e_1}(I_1)$ obtained by the procedure described in the proof of Lemma 6. By construction the entries of $I_0(\ell)$ and $I_1(\ell)$ are equal or differ by 1 and we will distinguish between two cases depending on the parity of the number of different entries.

Even case. *For any $\ell \in \{1,\dots,k\}$, $I_0(\ell)$ and $I_1(\ell)$ differ at an even number of entries.*

In this case, for any $\ell \in \{1,\dots,k\}$ we have $|I_0(\ell)| \equiv |I_1(\ell)| \bmod 2$, which implies

$$\left|T_1^{\mathbf{de}}(I)\right| + \cdots + \left|T_{k-1}^{\mathbf{de}'}(I)\right| \equiv \left|T_1^{\mathbf{de}}(I)\right| + \cdots + \left|T_{k-1}^{\mathbf{de}'}(I)\right| \bmod 2$$

and

$$\nu(I,\mathbf{d},\mathbf{e}) \equiv \nu(I,\mathbf{d},\mathbf{e}') + 1 \bmod 2,$$

so that Lemma 7 is true in this case.

Odd case. *There exists $\ell \in \{1,\dots,k\}$ such that $I_0(\ell)$ and $I_1(\ell)$ differ at an odd number of entries.*

In this case, let $\ell_0 \geq 1$ be the smallest number for which this occurs. In what follows we slightly modify the procedure described in the proof of Lemma 6 for the remaining steps. We again construct $(e_{\ell_0},\dots,e_{k-1})$ such that $T_k^{\mathbf{de}}(I) = T_k^{\mathbf{de}'}(I)$, but by using another principle, namely that at each step $\ell \geq \ell_0$ (with the only exception of the final steps) $I_0(\ell)$ and $I_1(\ell)$ differ at an odd number of positions. For convenience we say that a position j is corrected if $I_0(\ell+1)_{|j} = I_1(\ell+1)_{|j}$ whereas $I_0(\ell)_{|j}$ and $I_1(\ell)_{|j}$ differ by 1.

Let us describe the first step of this *new procedure*. When we compare $(T_{d_{\ell_0}0}(I_0(\ell_0)),\ T_{d_{\ell_0}0}(I_1(\ell_0)))$ and $(T_{d_{\ell_0}1}(I_0(\ell_0)),\ T_{d_{\ell_0}1}(I_1(\ell_0)))$, which are the possible candidates for $(I_0(\ell_0+1), I_1(\ell_0+1))$ it follows from Lemma 5 that a position j is corrected in the first case if and only if it is not corrected in the second case. This means that either $T_{d_{\ell_0}0}(I_0(\ell_0))$ and $T_{d_{\ell_0}0}(I_1(\ell_0))$ or $T_{d_{\ell_0}1}(I_0(\ell_0))$ and $T_{d_{\ell_0}1}(I_1(\ell_0))$ differ at an odd number of positions (and the other one at an even number of positions). Suppose without loss of generality that $T_{d_{\ell_0}0}(I_0(\ell_0)),\ T_{d_{\ell_0}0}(I_1(\ell_0))$ differs by an odd number of positions. If $T_{d_{\ell_0}1}(I_0(\ell_0)) = T_{d_{\ell_0}1}(I_1(\ell_0))$ then we choose $e_{\ell_0} = 1$ and the procedure stops. However, if $T_{d_{\ell_0+1}1}(I_0(\ell_0)) \neq T_{d_{\ell_0+1}1}(I_1(\ell_0))$ then we choose $e_{\ell_0} = 0$ and observe that the number of different positions in $I_0(\ell_0+1)$ and $I_1(\ell_0+1)$ is again odd but smaller than the number of different positions in $I_0(\ell_0)$ and $I_1(\ell_0)$. Of course we can proceed in this way step by step till $I_0(k) = I_1(k) = J$.

The advantage of this procedure is that we can control the values modulo 2 of $\nu(I,\mathbf{d},\mathbf{e})$ and $\nu(I,\mathbf{d},\mathbf{e}')$. Actually since $|I_0(\ell)| \equiv |I_1(\ell)| \bmod 2$ for $1 \le \ell < \ell_0$, $|I_0(\ell)| \not\equiv |I_1(\ell)| \bmod 2$ for $\ell_0 \le \ell \le m_0$ (with $1 \le m_0 < k$) and $I_0(\ell) = I_1(\ell) = J$ for $m_0 < \ell \le k$, we obtain

$$\nu(I,\mathbf{d},\mathbf{e}) \equiv \nu(I,\mathbf{d},\mathbf{e}') + (m_0 - \ell_0 + 1) + 1 \bmod 2.$$

If $m_0 - \ell_0$ is odd we are done.

If $m_0 - \ell_0$ is even we modify the last step of the above procedure. As $I_0(m_0)$ and $I_1(m_0)$ differ at an odd number of positions and $T_{d_{m_0}e_{m_0}}(I_0(m_0)) = T_{d_{m_0}e_{m_0}}(I_1(m_0))$, it follows, writing $\widetilde{e}_{m_0} = 1 - e_{m_0}$, that the number of different entries of $T_{d_{m_0}\widetilde{e}_{m_0}}(I_1(m_0))$ $T_{d_{m_0}\widetilde{e}_{m_0}}(I_0(m_0))$ is the same as the number of different entries of $I_0(m_0)$ and $I_1(m_0)$ (since $T_{d_{m_0}e_{m_0}}$ corrects all positions, $T_{d_{m_0}\widetilde{e}_{m_0}}$ corrects no position). By using $\widetilde{e}_{m_0}$ instead of e_{m_0} at step m_0, we have now that property that $I_0(m_0+1)$ and $I_1(m_0+1)$ differ at and odd number of positions.

If we can choose e_{m_0+1} in a way that $I_0(m_0+2) = I_1(m_0+2)$ then by the same arguments as above (where we have to replace m_0 by m_0+1) it follows that

$$\nu(I,\mathbf{d},\mathbf{e}) \equiv \nu(I,\mathbf{d},\mathbf{e}') + (m_0 + 1 - \ell_0 + 1) + 1 \bmod 2 \equiv \nu(I,\mathbf{d},\mathbf{e}') + 1 \bmod 2 \tag{46}$$

and we are done. In particular this is possible if $I_0(m_0+1)$ and $I_1(m_0+1)$ differ at precisely one position.

If we cannot choose e_{m_0+1} in a way that $I_0(m_0+2) = I_1(m_0+2)$ then we *restart* the original procedure at this point knowing that the number of different positions in $I_0(m_0+2)$ and $I_1(m_0+2)$ is smaller than the number of different positions in $I_0(m_0+1)$ and $I_1(m_0+1)$. If $I_0(\ell)$ and $I_1(\ell)$ differ at an even number of positions for all $\ell \ge m_0+2$ (till we end up at some common J), then we again get (46) and we are done. If not, let ℓ_1 be the smallest integer $\ell \ge m+1$ such that $I_0(\ell_1)$ and $I_1(\ell_1)$ differ at an odd number of positions. By construction this number is smaller that the number of different positions in $I_0(\ell_0)$ and $I_1(\ell_0)$ and we can proceed now by induction and the procedure will terminate after at most k steps. □

It is now easy to complete the proof of Proposition 2 by proving (42).

Lemma 8. *For any $\mathbf{d} \in \{0,1\}^{k+1}$, any $I \in \mathcal{I}_k$ and any $z \in \mathbb{U}$ we have*

$$\sum_{J \in \mathcal{I}_k} \left|P_{IJ}^{\mathbf{d}}(z)\right| < 2^{k+1}.$$

Proof. Lemmas 4 and 6 imply that for any $\mathbf{d} \in \{0,1\}^k$ and any $I \in \mathcal{I}_k$, there exists $J = J(I) \in \mathcal{I}_k$ and $j = j(I) \in \{0,\dots,2^k-2\}$ such that $\pm z^j$ and $\pm z^{j+1}$ are monomials of the polynomial $P_{IJ}^{\mathbf{d}}$. In particular, any $z \in \mathbb{U}$ such that $\sum_{J\in\mathcal{I}_k} \left|P_{IJ}^{\mathbf{d}}(z)\right| = 2^k$ should verify $|\pm z^j \pm z^{j+1}| = |z \pm 1| = 2$, which implies $z \in \{-1,+1\}$. Now Lemma 7 shows that we will actually find two consecutive terms of the form $\pm(z^j - z^{j+1})$ which implies that $z = 1$ can be excluded, too. Summing up we have proved that for all $I \in \mathcal{I}_k$ and all $z \in \mathbb{U} \setminus \{-1\}$ we have $\sum_{J\in\mathcal{I}_k} \left|P_{IJ}^{\mathbf{d}}(z)\right| < 2^k$.

Next we repeat the argument (however, just by using Lemma 6) by starting with any $\mathbf{d}' \in \{0,1\}^{k+1}$ and obtain that for all $I \in \mathcal{I}_k$ and all $z \in \mathbb{U} \setminus \{1,-1\}$ we have $\sum_{J\in\mathcal{I}_k} \left|P_{IJ}^{\mathbf{d}'}(z)\right| < 2^{k+1}$.

Now we set $\mathbf{d}' = (\varepsilon, d_0, \dots, d_{k-1})$ for $\varepsilon \in \{0,1\}$ so that we have $\mathbf{M}^{\mathbf{d}'}(z) = \mathbf{M}^{\varepsilon}(z)\mathbf{M}^{\mathbf{d}}(z^2)$ or

$$P_{IJ}^{\mathbf{d}'}(z) = (-1)^{|I|+\varepsilon\sigma} P_{T_{\varepsilon 0}(I)J}^{\mathbf{d}}(z^2) + (-1)^{|I|+\varepsilon\sigma+1} z P_{T_{\varepsilon 1}(I)J}^{\mathbf{d}}(z^2).$$

Since we have already observed that $\sum_{J\in\mathcal{I}_k} \left|P_{T_{\varepsilon,\varepsilon'}(I)J}^{\mathbf{d}}(1)\right| < 2^k$ we also have $\sum_{J\in\mathcal{I}_k} \left|P_{IJ}^{\mathbf{d}'}(\pm 1)\right| < 2^{k+1}$ which completes the proof of Lemma 8. □

8.2. **Proof of Proposition 2 in the case** $(\alpha_0,\dots,\alpha_{k-1})\neq(1,\dots,1)$**.** Without loss of generality we can assume that $\alpha_0=1$ and that for at least one $\ell\geq 1$ we have $\alpha_\ell=0$. As we mentionned in Section 7.2, the discrete Fourier transforms G_λ^I only depends on those indices ℓ for which $\alpha_\ell=1$, so that we again introduce the reduced K-uple $\tilde{I}=(i_\ell)_{0\leq\ell<k,\,\alpha_\ell=1}$ and the reduced sets $\tilde{\mathcal{I}}_k=\{\tilde{I},\ I\in\mathcal{I}_k\}$.

The proof of Proposition 2 works again in the case $(\alpha_0,\dots,\alpha_{k-1})\neq(1,\dots,1)$ in the same way as in the case $(\alpha_0,\dots,\alpha_{k-1})=(1,\dots,1)$ if we replace $\mathcal{I}_k$ by $\tilde{\mathcal{I}}_k$, G_λ^I by $G_\lambda^{\tilde{I}}$ and for any $(\varepsilon,\varepsilon')\in\{0,1\}^2$ the transformation $T_{\varepsilon\varepsilon'}$ on $\mathcal{I}_k$ by the corresponding transformation $\tilde{T}_{\varepsilon\varepsilon'}$ on $\tilde{\mathcal{I}}_k$. In particular we introduce, for any integer $m\geq 1$, $\mathbf{d}\in\{0,1\}^m$ and $z\in\mathbb{U}$, the matrices

$$\widetilde{\mathbf{M}}^{\mathbf{d}}(z)=\left(\widetilde{P}^{\mathbf{d}}_{\widetilde{I}\widetilde{J}}(z)\right)_{(\widetilde{I},\widetilde{J})\in\widetilde{\mathcal{I}}_k^2},$$

where the family of polynomials $\widetilde{P}^{\mathbf{d}}_{\widetilde{I}\widetilde{J}}$ verifies Lemma 4. The corresponding weighted directed graph $\widetilde{\mathcal{G}}(z)$ has still outdegree 4 but less vertices and the coefficients of the matrix $\widetilde{\mathbf{M}}^{\mathbf{d}}(z)$ can still be interpreted as codings of path of length m with, for $j\in\{0,\dots,m-1\}$, step j in the graph $\widetilde{\mathcal{G}}(z^{2^j})$. More precisely, for any $\widetilde{I}\in\widetilde{\mathcal{I}}_k$, $\mathbf{e}=(e_0,\dots,e_{m-1})\in\{0,1\}^m$ and $i\in\{1,\dots,m\}$, if we denote $\tilde{T}_i^{\mathbf{de}}(\widetilde{I})=\tilde{T}_{d_{i-1}e_{i-1}}\circ\cdots\circ\tilde{T}_{d_0e_0}(\widetilde{I})$ we can associate to each of the 2^m paths from the vertex $\widetilde{I}$ to the vertices $\tilde{T}_m^{\mathbf{de}}(\widetilde{I})$ the weight

$$\begin{aligned}w^{\mathbf{de}}(\widetilde{I},z)&=w_{d_0e_0}(\widetilde{I},z)w_{d_1e_1}(\tilde{T}_1^{\mathbf{de}}(\widetilde{I}),z^2)\cdots w_{d_{m-1}e_{m-1}}(\tilde{T}_{m-1}^{\mathbf{de}}(\widetilde{I}),z^{2^{m-1}})\\&=(-1)^{\nu(\widetilde{I},\mathbf{d},\mathbf{e})}z^{N(\mathbf{e})},\end{aligned}$$

so that, for any $(\widetilde{I},\widetilde{J})\in\widetilde{\mathcal{I}}_k^2$, we have, by definition of $\widetilde{P}^{\mathbf{d}}_{\widetilde{I}\widetilde{J}}$:

$$\widetilde{P}^{\mathbf{d}}_{\widetilde{I}\widetilde{J}}(z)=\sum_{\substack{\mathbf{e}\in\{0,1\}^m\\ \tilde{T}_m^{\mathbf{de}}(\widetilde{I})=\widetilde{J}}}w^{\mathbf{de}}(\widetilde{I},z)=\sum_{\substack{\mathbf{e}\in\{0,1\}^m\\ \tilde{T}_m^{\mathbf{de}}(\widetilde{I})=\widetilde{J}}}(-1)^{\nu(\widetilde{I},\mathbf{d},\mathbf{e})}z^{N(\mathbf{e})}.$$

Next, the Lemmas 5, 6, and 7 can be generalized in a direct way, replacing I by $\tilde{I}$, $\mathcal{I}_k$ by $\tilde{\mathcal{I}}_k$ and for any $m\in\{1,\dots,k\}$ and any $(\mathbf{d},\mathbf{e})\in\{0,1\}^m\times\{0,1\}^m$, $T_m^{\mathbf{de}}$ by $\tilde{T}_m^{\mathbf{de}}$. In particular the procedures described in Lemmas 6, and 7 directly translate to this case. For example we can project the two paths from the proof of Lemma 6 that connect I to J to corresponding paths that connect $\tilde{I}$ and $\tilde{J}$ and prove that for any $m\geq k$, $\mathbf{d}\in\{0,1\}^m$ and $\widetilde{I}\in\widetilde{\mathcal{I}}_k$ there exist $\widetilde{J}\in\widetilde{\mathcal{I}}_k$ such that the polynomial $\widetilde{P}^{\mathbf{d}}_{\widetilde{I}\widetilde{J}}$ contains two monomials of consecutive degrees and then show, as in Lemma 7, that we can find $\widetilde{J}\in\widetilde{\mathcal{I}}_k$ such that the polynomial $\widetilde{P}^{\mathbf{d}}_{\widetilde{I}\widetilde{J}}$ contains two monomials of consecutive degrees and opposite signs by distinguish again an even case and an odd case.

This completes the proof of Proposition 2.

9. Auxiliary Lemmas

9.1. **A multidimensional application of Beurling-Selberg-Vaaler's method.** For $\alpha\in\mathbb{R}$ with $0\leq\alpha<1$ let χ_α be the characteristic function of the interval $[0,\alpha)$ modulo 1 defined by (6). The following lemma is a classical way to detect real numbers in an interval modulo 1 by means of exponential sums.

Lemma 9. *For all $\alpha\in\mathbb{R}$ with $0\leq\alpha<1$ and all integer $H\geq 1$ there exist real valued trigonometric polynomials $A_{\alpha,H}(x)$ and $B_{\alpha,H}(x)$ such that for all $x\in\mathbb{R}$*

$$|\chi_\alpha(x)-A_{\alpha,H}(x)|\leq B_{\alpha,H}(x), \tag{47}$$

where

$$A_{\alpha,H}(x)=\sum_{|h|\le H} a_h(\alpha,H)\,\mathrm{e}(hx),\ B_{\alpha,H}(x)=\sum_{|h|\le H} b_h(\alpha,H)\,\mathrm{e}(hx), \tag{48}$$

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

$$a_0(\alpha,H)=\alpha,\ |a_h(\alpha,H)|\le \min\left(\alpha,\tfrac{1}{\pi|h|}\right),\ |b_h(\alpha,H)|\le \tfrac{1}{H+1}. \tag{49}$$

Proof. This is a consequence of Theorem 19 of [28] (see also the proof of [22, Lemma 1]). . □

Similarly we can detect points in a d-dimensional box (modulo 1):

Lemma 10. *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* $(x_1,\dots,x_d)\in\mathbb{R}^d$

$$\left|\prod_{j=1}^d \chi_{\alpha_j}(x_j)-\prod_{j=1}^d A_{\alpha_j,H_j}(x_j)\right|\le \sum_{\emptyset\ne J\subseteq\{1,\dots,d\}}\ \prod_{j\notin J}\chi_{\alpha_j}(x_j)\prod_{j\in J}B_{\alpha_j,H_j}(x_j) \tag{50}$$

where $A_{\alpha,H}(.)$ *and* $B_{\alpha,H}(.)$ *are the real valued trigonometric polynomials defined by* (48).

Proof. We have

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

Since $\chi_{\alpha_i}\ge 0$, by (47) we get (50). □

Lemma 11. *Let* $\mathcal{N}$ *be a finite set and* $f_1:\mathcal{N}\to\mathbb{R},\ \dots,\ f_d:\mathcal{N}\to\mathbb{R}$. *Let* $U_1\ge 1,\ \dots,U_d\ge 1$ *be integers and*

$$g:\mathcal{N}\times\{0,\dots,U_1-1\}\times\cdots\times\{0,\dots,U_d-1\}\to\mathbb{C}$$

such that $|g|\le 1$. *The sum*

$$S=\sum_{n\in\mathcal{N}}\sum_{0\le u_1<U_1}\cdots\sum_{0\le u_d<U_d} g(n,u_1,\dots,u_d)\ \prod_{j=1}^d \chi_{U_j^{-1}}\left(f_j(n)-\frac{u_j}{U_j}\right)$$

can be approximated, for any integers $H_1\ge 1,\ \dots,\ H_d\ge 1$, *by*

$$\widetilde{S}=\sum_{\substack{|h_1|\le H_1\\ \cdots\\ |h_d|\le H_d}} a_{h_1}(U_1^{-1},H_1)\cdots a_{h_d}(U_d^{-1},H_d)\sum_{\substack{0\le u_1<U_1\\ \cdots\\ 0\le u_d<U_d}}\mathrm{e}\left(-\frac{h_1u_1}{U_1}-\cdots-\frac{h_du_d}{U_d}\right)$$
$$\sum_{n\in\mathcal{N}} g(n,u_1,\dots,u_d)\,\mathrm{e}\left(h_1f_1(n)+\cdots+h_df_d(n)\right)$$

with the error estimate:

$$\left|S-\widetilde{S}\right|\le\sum_{\ell=1}^d\ \sum_{1\le j_1<\cdots<j_\ell\le d} E_{j_1,\dots,j_\ell} \tag{51}$$

with $E_{j_1,\dots,j_\ell}$ *defined by*

$$\frac{U_{j_1}\cdots U_{j_\ell}}{(H_{j_1}+1)\cdots(H_{j_\ell}+1)}\sum_{\substack{|h_{j_1}|\le H_{j_1}/U_{j_1}\\ \cdots\\ |h_{j_\ell}|\le H_{j_\ell}/U_{j_\ell}}}\left|\sum_{n\in\mathcal{N}}\mathrm{e}\left(h_{j_1}U_{j_1}f_{j_1}(n)+\cdots+h_{j_\ell}U_{j_\ell}f_{j_\ell}(n)\right)\right|.$$

Proof. We have

$$S-\widetilde{S}=\sum_{n\in\mathcal{N}}\sum_{\substack{0\le u_1<U_1\\ \cdots\\ 0\le u_d<U_d}} g(n,u_1,\dots,u_d)\left(\prod_{j=1}^{d}\chi_{U_j^{-1}}\left(f_j(n)-\frac{u_j}{U_j}\right)-\prod_{j=1}^{d}A_{U_j^{-1},H_j}\left(f_j(n)-\frac{u_j}{U_j}\right)\right).$$

Using (50) and the hypothesis $|g|\le 1$ we obtain

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

For any $t\in\mathbb{R}$, we have

$$\sum_{0\le u_j<U_j}\chi_{U_j^{-1}}\left(t-\frac{u_j}{U_j}\right)=1,$$

which shows that the first parenthesis is equal to 1. Observing that

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

we can write

$$\begin{aligned}\sum_{0\le u_j<U_j}B_{U_j^{-1},H_j}\left(f_j(n)-\frac{u_j}{U_j}\right)&=\sum_{0\le u_j<U_j}\sum_{|h_j|\le H_j}b_{h_j}(U_j^{-1},H_j)\,\mathrm{e}\left(h_jf_j(n)-\frac{h_ju_j}{U_j}\right)\\&=U_j\sum_{|h_j|\le H_j/U_j}b_{h_jU_j}(U_j^{-1},H_j)\,\mathrm{e}\left(h_jU_jf_j(n)\right),\end{aligned}$$

which leads to

$$\left|S-\widetilde{S}\right|\le\sum_{\emptyset\neq J\subseteq\{1,\dots,d\}}\sum_{n\in\mathcal{N}}\prod_{j\in J}\left(U_j\sum_{|h_j|\le H_j/U_j}b_{h_jU_j}(U_j^{-1},H_j)\,\mathrm{e}\left(h_jU_jf_j(n)\right)\right).$$

Expanding the product, reversing the order of summations and then using $\left|b_{h_jU_j}(U_j^{-1},H_j)\right|\le(H_j+1)^{-1}$ (by (49)) this leads to (51). □

9.2. **Generalized van der Corput's inequality.**

Lemma 12. *For all complex numbers $z_1,\dots,z_N$ and all integers $Q\ge 1$ and $R\ge 1$ we have*

$$\left|\sum_{1\le n\le N}z_n\right|^2\le\frac{N+QR-Q}{R}\left(\sum_{1\le n\le N}|z_n|^2+2\sum_{1\le r<R}\left(1-\frac{r}{R}\right)\sum_{1\le n\le N-Qr}\Re\left(z_{n+Qr}\overline{z_n}\right)\right)\tag{52}$$

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

Proof. See for example Lemma 17 of [20]. □

9.3. **Sums of geometric series.** We will often make use of the following upper bound of geometric series of ratio $\mathrm{e}(\xi)$ for $(L_1,L_2)\in\mathbb{Z}^2$, $L_1\le L_2$ and $\xi\in\mathbb{R}$:

$$\left|\sum_{L_1<\ell\le L_2}\mathrm{e}(\ell\xi)\right|\le\min(L_2-L_1,|\sin\pi\xi|^{-1}).\tag{53}$$

Lemma 13. *Let $(a,m)\in\mathbb{Z}^2$ with $m\geq 1$, $\delta=\gcd(a,m)$ and $b\in\mathbb{R}$. For any real number $U>0$ we have*

$$\sum_{0\leq n\leq m-1}\min\Big(U,\big|\sin\pi\tfrac{an+b}{m}\big|^{-1}\Big)\leq \delta\min\Big(U,\Big|\sin\pi\tfrac{\delta\,\|b/\delta\|}{m}\Big|^{-1}\Big)+\frac{2\,m}{\pi}\log(2\,m). \tag{54}$$

Proof. The result is trivial for $m=1$. For $m\geq 2$ after using Lemma 6 of [21] it suffices to observe that

$$\frac{\delta}{\sin\frac{\pi\delta}{2m}}+\frac{2m}{\pi}\log\frac{2m}{\pi\delta}\leq\frac{1}{\sin\frac{\pi}{2m}}+\frac{2m}{\pi}\log\frac{2m}{\pi}\leq\frac{2\,m}{\pi}\log(2\,m).$$

□

Lemma 14. *Let $m\geq 1$ and $A\geq 1$ be integers and $b\in\mathbb{R}$. For any real number $U>0$ we have*

$$\frac{1}{A}\sum_{1\leq a\leq A}\sum_{0\leq n<m}\min\Big(U,\big|\sin\pi\tfrac{an+b}{m}\big|^{-1}\Big)\ll\tau(m)\;U+m\log m \tag{55}$$

and if $|b|\leq\frac12$ we have the sharper bound

$$\frac{1}{A}\sum_{1\leq a\leq A}\sum_{0\leq n<m}\min\Big(U,\big|\sin\pi\tfrac{an+b}{m}\big|^{-1}\Big)\ll\tau(m)\min\Big(U,\big|\sin\pi\tfrac{b}{m}\big|^{-1}\Big)+m\log m, \tag{56}$$

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

Proof. Using (54) we have for all $b\in\mathbb{R}$:

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

while for $|b|\leq\frac12$, since $\gcd(a,m)\,\|b/\gcd(a,m)\|=|b|$ this can be sharpened using (54) to

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

Now

$$\sum_{1\leq a\leq A}\gcd(a,m)=\sum_{\substack{d\,|\,m\\ d\leq A}}d\sum_{\substack{1\leq a\leq A\\ \gcd(a,m)=d}}1\leq\sum_{\substack{d\,|\,m\\ d\leq A}}d\sum_{\substack{1\leq a\leq A\\ d\,|\,a}}1=\sum_{\substack{d\,|\,m\\ d\leq A}}d\left\lfloor\frac{A}{d}\right\rfloor\leq A\;\tau(m) \tag{57}$$

which implies (55) and (56) when $|b|\leq\frac12$. □

9.4. **Gauss sums.**

Lemma 15. *For all $(a,b,m)\in\mathbb{Z}^3$ with $m\geq 1$, we have*

$$\left|\sum_{n=0}^{m-1}\mathrm{e}\left(\tfrac{an^2+bn}{m}\right)\right|\leq\sqrt{2m\gcd(a,m)}. \tag{58}$$

Proof. This is Proposition 2 of [20] (notice that $\gcd(0,m)=m$). □

For incomplete quadratic Gauss sums we have

Lemma 16. *For all $(a,b,m,N,n_0)\in\mathbb{Z}^5$ with $m\geq 1$ and $N\geq 0$, we have*

$$\left|\sum_{n=n_0+1}^{n_0+N}\mathrm{e}\left(\tfrac{an^2+bn}{m}\right)\right|\leq\big(\tfrac{N}{m}+1+\tfrac{2}{\pi}\log\tfrac{2m}{\pi}\big)\sqrt{2m\gcd(a,m)}. \tag{59}$$

Proof. The following argument is a variant of a method known at least since Vinogradov. For $m = 1$ the result is true. Assume that $m \geq 2$. There are $\lfloor N/m \rfloor$ complete sums which are bounded above by $\sqrt{2m \gcd(a, m)}$. The remaining sum is either empty or of the form

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

for some $n_1 \in \mathbb{Z}$ and $1 \leq L \leq m$. We have

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

hence

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

thus

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

Applying Lemma 15 with b replaced by $b+k$ and observing (by convexity of $t \mapsto 1/\sin(\pi t/m)$) that

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

we obtain (59). □

9.5. **Norm of matrix products.** We denote by $\|\mathbf{A}\|_\infty = \max_{1 \leq i \leq N} \sum_{j=1}^N |A_{i,j}|$ the row-sum norm of a matrix $\mathbf{A} = (A_{i,j})_{(i,j) \in \{1,\dots,N\}^2}$.

Lemma 17. *Let $\mathbf{M}_\ell$, $\ell \in \mathbb{N}$, be $N \times N$-matrices with complex entries $M_{\ell;i,j}$, $1 \leq i, j \leq N$, and absolute row sums*

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

Furthermore assume that there exists integers $m_0 \geq 1$ and $m_1 \geq 1$ and constants $c_0 > 0$ and $\eta > 0$ such that

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

$$|A_{i,1}| \geq c_0 \quad \text{or} \quad \sum_{j=1}^N |A_{i,j}| \leq 1 - \eta;$$

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

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

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

$$\left\| \prod_{\ell=r}^{r+k-1} \mathbf{M}_\ell \right\|_\infty \leq C 2^{-\delta k} \tag{60}$$

uniformly for all $r \geq 0$ and $k \geq 0$.

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

$$\left\| \prod_{\ell=r}^{r+k-1} \mathbf{M}_\ell \right\|_\infty \le (1-\eta c_0)^{\lfloor k/(m_0+m_1)\rfloor} \le \frac{1}{1-\eta c_0}\, 2^{-\eta c_0 k/(m_0+m_1)}$$

and we obtain (60) for $C = 1/(1-\eta c_0)$ and $\delta = \eta c_0/(m_0+m_1)$.

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

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

Similarly if we have $\sum_{j=1}^N |A_{i,j}| \le 1-\eta$ then

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

Since $c_0 \le 1$ we have $1-\eta \le 1 - c_0\eta$, which completes the proof of Lemma 17. □

Acknowledgements. We thank the referee for his careful reading and his valuable remarks.

References

[1] J.-P. Allouche and J. Shallit, *Automatic sequences*, Cambridge University Press, Cambridge, 2003. Theory, applications, generalizations.

[2] A. Bellow, *Two problems*, in Measure Theory, Proceedings of the Conference held at Oberwolfach, June 21-27, 1981, no. 945 in Lecture Notes in Mathematics, Springer Verlag, 1982.

[3] V. Bergelson and A. Leibman, *Polynomial extensions of van der Waerden's and Szemerédi's theorems*, J. Amer. Math. Soc., 9 (1996), pp. 725–753.

[4] E. Borel, *Les probabilités dénombrables et leurs applications arithmétiques.*, Rend. Circ. Mat. Palermo, 27 (1909), pp. 247–271.

[5] J. Bourgain, *On the maximal ergodic theorem for certain subsets of the integers*, Israel J. Math., 61 (1988), pp. 39–72.

[6] ——, *On the pointwise ergodic theorem on L^p for arithmetic sets*, Israel J. Math., 61 (1988), pp. 73–84.

[7] ——, *Pointwise ergodic theorems for arithmetic sets*, Inst. Hautes Études Sci. Publ. Math., (1989), pp. 5–45. With an appendix by the author, Harry Furstenberg, Yitzhak Katznelson and Donald S. Ornstein.

[8] S. Brlek, *Enumeration of factors in the Thue-Morse word*, Discrete Appl. Math., 24 (1989), pp. 83–96. First Montreal Conference on Combinatorics and Computer Science, 1987.

[9] Z. Buczolich and R. D. Mauldin, *Divergent square averages*, Ann. of Math. (2), 171 (2010), pp. 1479–1530.

[10] Y. Bugeaud, *Distribution modulo one and Diophantine approximation*, vol. 193 of Cambridge Tracts in Mathematics, Cambridge University Press, Cambridge, 2012.

[11] D. Champernowne, *The construction of decimals normal in the scale of ten.*, J. Lond. Math. Soc., 8 (1933), pp. 254–260.

[12] A. Cobham, *Uniform tag sequences*, Math. Systems Theory, 6 (1972), pp. 164–192.

[13] A. de Luca and S. Varricchio, *Some combinatorial properties of the Thue-Morse sequence and a problem in semigroups*, Theoret. Comput. Sci., 63 (1989), pp. 333–348.

[14] H. Furstenberg, *Problem session*, Conference on Ergodic Theory and Applications, University of New Hampshire, Durham, NH, June 1982, (1982).
[15] W. H. Gottschalk and G. A. Hedlund, *A characterization of the Morse minimal set*, Proc. Amer. Math. Soc., 15 (1964), pp. 70–74.
[16] B. Host and B. Kra, *Convergence of polynomial ergodic averages*, Israel J. Math., 149 (2005), pp. 1–19. Probability in mathematics.
[17] ——, *Nonconventional ergodic averages and nilmanifolds*, Ann. of Math. (2), 161 (2005), pp. 397–488.
[18] P. Kůrka, *Topological and symbolic dynamics.*, Paris: Société Mathématique de France, 2003.
[19] C. Mauduit, *Multiplicative properties of the Thue-Morse sequence*, Period. Math. Hungar., 43 (2001), pp. 137–153.
[20] C. Mauduit and J. Rivat, *La somme des chiffres des carrés*, Acta Math., 203 (2009), pp. 107–148.
[21] ——, *Sur un problème de Gelfond: la somme des chiffres des nombres premiers*, Ann. of Math. (2), 171 (2010), pp. 1591–1646.
[22] ——, *Prime numbers along Rudin-Shapiro sequences*, J. Eur. Math. Soc. (JEMS), 17 (2015), pp. 2595–2642.
[23] H. M. Morse, *Recurrent geodesics on a surface of negative curvature*, Trans. Amer. Math. Soc., 22 (1921), pp. 84–100.
[24] Y. Moshe, *On the subword complexity of Thue-Morse polynomial extractions*, Theoret. Comput. Sci., 389 (2007), pp. 318–329.
[25] N. Pytheas Fogg, *Substitutions in dynamics, arithmetics and combinatorics*, vol. 1794 of Lecture Notes in Mathematics, Springer-Verlag, Berlin, 2002. Edited by V. Berthé, S. Ferenczi, C. Mauduit and A. Siegel.
[26] M. Queffelec, *Substitution Dynamical Systems – Spectral Analysis*, vol. 1294 of Lecture Notes in Math., Springer Verlag, New-York – Berlin, 1987.
[27] A. Thue, *Über die gegenseitige Lage gleicher Teile gewisser Zeichenreihen.* Kristiania: J. Dybwad. 67 S. Lex. 8° (1912)., 1912.
[28] J. Vaaler, *Some extremal functions in Fourier analysis*, Bull. Amer. Math. Soc., 12 (1985), pp. 183–216.
[29] T. Ziegler, *Universal characteristic factors and Furstenberg averages*, J. Amer. Math. Soc., 20 (2007), pp. 53–97 (electronic).

E-mail address: michael.drmota@tuwien.ac.at

Institut für Diskrete Mathematik und Geometrie TU Wien, Wiedner Hauptstr. 8–10, 1040 Wien, Austria

E-mail address: mauduit@iml.univ-mrs.fr

Université d'Aix-Marseille and Institut Universitaire de France, Institut de Mathématiques de Marseille, CNRS UMR 7373, 163, avenue de Luminy, Case 907, 13288 MARSEILLE Cedex 9, France

E-mail address: joel.rivat@univ-amu.fr

Université d'Aix-Marseille, Institut de Mathématiques de Marseille, CNRS UMR 7373, 163, avenue de Luminy, Case 907, 13288 MARSEILLE Cedex 9, France