THE THUE-MORSE SEQUENCE ALONG SQUARES IS NORMAL

MICHAEL DRMOTA, CHRISTIAN MAUDUIT, AND JOËL RIVAT

Abstract. The Thue-Morse sequence is a classical example of an almost periodic (or uniformly recurrent) sequence in the sense that its associated symbolic dynamical system is minimal. We prove that the subsequence along squares of the Thue-Morse sequence is normal.

1. Introduction

The goal of this work is to show a first example of an almost periodic 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.

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 taking strictly positive values such that f/g is bounded, 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 $\mathbf{t} = (t(n))_{n\in\mathbb{N}} \in \{0,1\}^{\mathbb{N}}$. For example it is easy the check that $\mathbf{t}$ is the fixed point of the substitution $0 \to 01$ and $1 \to 10$ with $t(0) = 0$ and 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 [17] and by Morse in [12] (see also [14] for an earlier variant introduced by Prouhet), the Thue-Morse sequence has been studied in many different contexts from combinatorics to algebra, number theory, harmonic analysis, geometry and dynamical systems (see [1, 8]).

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.*

Date: October 19, 2013.

2000 *Mathematics Subject Classification.* Primary: 11A63, 11L03, 11N05, Secondary: 11N60, 11L20, 60F05.

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

This work was supported by the Agence Nationale de la Recherche project ANR-10-BLAN 0103 called MUNUM.

Morse proved in [12] that $\mathbf{t}$ is an almost periodic sequence (see also [8, Proposition 4] or [15, 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 [16, Theorem IV.12] or [15, Proposition 5.1.13]).

1.2. **Low complexity of the Thue-Morse sequence.**

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

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

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

It follows from Definition 3 that for any sequence $\mathbf{u}$ the function $p_{\mathbf{u}}$ verifies $1 \le p_{\mathbf{u}}(k) \le 2^k$ and 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 [7]).

The sequence $\mathbf{t}$ is defined by a very simple algorithm and its symbolic complexity is very low: it follows from [3, Proposition 4.5] or [6, Corollary 4.5] that for any positive integer k we have $p_{\mathbf{t}}(k) \le \frac{10}{3}k$. 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 [2] 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 also sublinear: $p_{\mathbf{t}_{a,b}}(k) = O_a(k)$ (see [5, 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 $\mathbf{u} \in \{0,1\}^{\mathbb{N}}$ is normal if, for any $k \in \mathbb{N}$ and any $(b_0, \dots, b_{k-1}) \in \{0,1\}^k$, we have*

$$\lim_{N\to\infty} \frac{1}{N} \mathrm{card}\{i < N,\ u(i) = b_0, \dots, u(i+k-1) = b_{k-1}\} = \frac{1}{2^k}.$$

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

There are only few known explicit constructions of normal numbers in a given base (see [4, Chapters 4 and 5]). This theorem provided a new construction of a number normal in base 2.

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

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

$$\forall n \in \mathbb{N},\ t^{(q)}(n) = \mathrm{s}(n^2) \bmod q.$$

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

Allouche and Shallit conjectured in [2, Problem 10.12.7] that the symbolic complexity of the sequence $\mathbf{t_2}$ is maximal (*i.e.* that for any positive integer k, we have $p_{\mathbf{t_2}}(k) = 2^k$) and this

conjecture was proved by Moshe in [13]. The control of the frequency of occurency of the blocks of length k is a more difficult question. When $k = 1$, it follows from [9] that

$$\lim_{N\to\infty} \frac{1}{N} \operatorname{card}\{n < N,\ t(n^2) = 0\} = \lim_{N\to\infty} \frac{1}{N} \operatorname{card}\{n < N,\ t(n^2) = 1\} = \frac{1}{2},$$

but the method of [9] does not allow to control higher order correlations. In this work we introduce new ideas in order to be able to control the Fourier transform of correlations of any order.

2. Plan of the Proof

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

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

For $(\lambda, \mu) \in \mathbb{N}^2$ such that $0 \leq \mu < \lambda$, we define the truncated binary sum-of-digits function s_λ and the two-fold restricted binary sum of digits function $\mathrm{s}_{\mu,\lambda}$ by

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

We also write

$$f_\lambda(n) = \tfrac{1}{2}\,\mathrm{s}_\lambda(n) \quad \text{and} \quad f_{\mu,\lambda}(n) = \tfrac{1}{2}\,\mathrm{s}_{\mu,\lambda}(n).$$

In order to prove our main result, we actually need the following theorem on exponential sums.

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

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

Lemma 1. *Theorem 2 implies that the sequence $\mathbf{t_2}$ is normal.*

Proof. Let $(b_0, \ldots, b_{k-1}) \in \{0, 1\}^k$. Then by assuming that (1) holds we obtain

$$\begin{aligned}
&\operatorname{card}\{n < N : (t_{n^2}, \ldots, t_{(n+k-1)^2}) = (b_0, \ldots, b_{k-1})\} \\
&= \sum_{n<N} \mathbf{1}_{[t_{n^2}=b_0]} \cdots \mathbf{1}_{[t_{(n+k-1)^2}=b_{k-1}]} \\
&= \sum_{n<N} \frac{1}{2} \sum_{\alpha_0=0}^{1} \mathrm{e}\left(\frac{\alpha_0}{2}\left(\mathrm{s}(n^2) - b_0\right)\right) \cdots \frac{1}{2} \sum_{\alpha_{k-1}=0}^{1} \mathrm{e}\left(\frac{\alpha_{k-1}}{2}\left(\mathrm{s}((n+k-1)^2) - b_{k-1}\right)\right) \\
&= \frac{1}{2^k} \sum_{(\alpha_0,\ldots,\alpha_{k-1})\in\{0,1\}^k} \mathrm{e}\left(-\frac{\alpha_0 b_0 + \cdots + \alpha_{k-1} b_{k-1}}{2}\right) \sum_{n<N} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \frac{1}{2} \alpha_\ell\, \mathrm{s}((n+\ell)^2)\right) \\
&= \frac{N}{2^k} + O\left(N^{1-\eta}\right)
\end{aligned}$$

with $\eta > 0$ obtained in Theorem 2. □

Thus, we just have to concentrate on Theorem 2. The structure of the full proof of Theorem 2 is the following one. First we collect some auxiliary results (Section 3). The following Section 4 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

$$G_\lambda^I(h,d) = \frac{1}{2^\lambda} \sum_{0\le u<2^\lambda} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell f_\lambda(u+\ell d+i_\ell) - h2^{-\lambda}\right),$$

where $I=(i_0,\dots,i_{k-1})\in\mathbb{N}^k$. 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 exponential sums. The corresponding bounds are formulated in Propositions 1 and 2 (see Section 5) and proved in Sections 8 and 9. 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 6 and 7 correspond to this distinction. In Section 6 we prove that if K is even we can deduce Theorem 2 from Proposition 1 and in Section 7 we prove that if K is odd we can deduce Theorem 2 from Proposition 2. Finally, the last two sections (Sections 8 and 9) provide the proofs of Propositions 1 and 2. Proposition 1 is a bound on averages of Fourier transforms and is actually much easier to prove than the uniform bound of Proposition 2 which is needed in the odd case.

3. Auxiliary Lemmas

3.1. **A multidimensional application of Vaaler's method.** The following lemma is a classical method to detect real numbers in an interval modulo 1 by means of exponential sums. For $\alpha\in\mathbb{R}$ with $0\le\alpha<1$ we denote by χ_α the characteristic function of the interval $[0,\alpha)$ modulo 1:

$$\chi_\alpha(x) = \lfloor x\rfloor - \lfloor x-\alpha\rfloor. \tag{2}$$

Lemma 2. *For all $\alpha\in\mathbb{R}$ with $0\le\alpha<1$ and all integer $H\ge1$ there exist real valued trigonometric polynomials $A_{\alpha,H}(x)$ and $B_{\alpha,H}(x)$ such that for all $x\in\mathbb{R}$*

$$|\chi_\alpha(x) - A_{\alpha,H}(x)| \le B_{\alpha,H}(x), \tag{3}$$

where

$$A_{\alpha,H}(x) = \sum_{|h|\le H} a_h(\alpha,H)\,\mathrm{e}(hx),\ B_{\alpha,H}(x) = \sum_{|h|\le H} b_h(\alpha,H)\,\mathrm{e}(hx), \tag{4}$$

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

$$a_0(\alpha,H)=\alpha,\ |a_h(\alpha,H)|\le\min\left(\alpha,\tfrac{1}{\pi|h|}\right),\ |b_h(\alpha,H)|\le\tfrac{1}{H+1}. \tag{5}$$

Proof. This is a consequence of Theorem 19 of [18] (see [11, Lemma 1]). □

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

Lemma 3. *For $(\alpha_1,\dots,\alpha_d)\in[0,1)^d$ and $(H_1,\dots,H_d)\in\mathbb{N}^d$ with $H_1\ge1,\dots,\ H_d\ge1$, we have for all $(x_1,\dots,x_d)\in\mathbb{R}^d$*

$$\left|\prod_{j=1}^d \chi_{\alpha_j}(x_j) - \prod_{j=1}^d A_{\alpha_j,H_j}(x_j)\right| \le \sum_{\emptyset\ne J\subsetneq\{1,\dots,d\}} \prod_{j\notin J}\chi_{\alpha_j}(x_j)\prod_{j\in J} B_{\alpha_j,H_j}(x_j) \tag{6}$$

where $A_{\alpha,H}(.)$ and $B_{\alpha,H}(.)$ are the real valued trigonometric polynomials defined by (4).

Proof. We have

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

Since $\chi_{\alpha_i}\geq 0$, by (3) we get (6). □

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

$$\sum_{0\leq u_j<U_j}\chi_{\alpha_j}\left(x-\frac{u_j}{U_j}\right)=1, \tag{7}$$

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

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

as

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

Let $(H_1,\dots,H_d)\in\mathbb{N}^d$ with $H_1\geq 1,\dots,H_d\geq 1$ and

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

Lemma 4. *With the above notations we have*

$$\left|S-\widetilde{S}\right|\leq\sum_{\ell=1}^{d-1}\sum_{1\leq j_1<\dots<j_\ell}\frac{U_{j_1}\cdots U_{j_\ell}}{H_{j_1}\cdots H_{j_\ell}}\sum_{|h_{j_1}|\leq H_{j_1}/U_{j_1}}\cdots\sum_{|h_{j_\ell}|\leq H_{j_\ell}/U_{j_\ell}}\left|\sum_{n=1}^{N}\mathrm{e}\left(h_{j_1}U_{j_1}f_{j_1}(n)+\dots+h_{j_\ell}U_{j_\ell}f_{j_\ell}(n)\right)\right|. \tag{8}$$

Proof. By (6) we have

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

which by (7) gives

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

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

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

Observing that

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

we obtain

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

Expanding the product, reversing the order of summations and using (5) this leads to (8). □

3.2. **Van der Corput's inequality.** The following lemma is a generalization of van der Corput's inequality.

Lemma 5. *For all complex numbers $z_1,\dots,z_N$ and all integers $Q\ge 1$ and $R\ge 1$ we have*

$$\left|\sum_{1\le n\le N} z_n\right|^2 \le \frac{N+QR-Q}{R}\left(\sum_{1\le n\le N}|z_n|^2 + 2\sum_{1\le r<R}\left(1-\frac{r}{R}\right)\sum_{1\le n\le N-Qr}\Re\left(z_{n+Qr}\overline{z_n}\right)\right) \tag{9}$$

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

Proof. See for example Lemma 17 of [9]. □

3.3. **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 $\xi\in\mathbb{R}$:

$$\left|\sum_{L_1<\ell\le L_2}\mathrm{e}(\ell\xi)\right| \le \min(L_2-L_1,|\sin\pi\xi|^{-1}). \tag{10}$$

Lemma 6. *Let $(a,m)\in\mathbb{Z}^2$ with $m\ge 1$, $\delta=\gcd(a,m)$ and $b\in\mathbb{R}$. For any real number $U>0$ we have*

$$\sum_{0\le n\le m-1}\min\left(U,\left|\sin\pi\tfrac{an+b}{m}\right|^{-1}\right) \le \delta\min\left(U,\left|\sin\pi\tfrac{\delta\,\|b/\delta\|}{m}\right|^{-1}\right)+\frac{2\,m}{\pi}\log(2\,m). \tag{11}$$

Proof. The result is trivial for $m=1$. For $m\ge 2$ after using Lemma 6 of [10] it suffice to observe that

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

□

Lemma 7. *Let $m\ge 1$ and $A\ge 1$ be integers and $b\in\mathbb{R}$. For any real number $U>0$ we have*

$$\frac{1}{A}\sum_{1\le a\le A}\sum_{0\le n<m}\min\left(U,\left|\sin\pi\tfrac{an+b}{m}\right|^{-1}\right) \ll \tau(m)\;U+m\log m \tag{12}$$

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

$$\frac{1}{A}\sum_{1\le a\le A}\sum_{0\le n<m}\min\left(U,\left|\sin\pi\tfrac{an+b}{m}\right|^{-1}\right) \ll \tau(m)\min\left(U,\left|\sin\pi\tfrac{b}{m}\right|^{-1}\right)+m\log m, \tag{13}$$

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

Proof. Using (11) we have for all $b \in \mathbb{R}$:

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

while for $|b| \le \frac{1}{2}$, since $\gcd(a,m)\,\|b/\gcd(a,m)\| = |b|$ this can be sharpened using (11) to

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

Now

$$\sum_{1\le a\le A} \gcd(a,m) = \sum_{\substack{d\,|\,m\\ d\le A}} d \sum_{\substack{1\le a\le A\\ \gcd(a,m)=d}} 1 \le \sum_{\substack{d\,|\,m\\ d\le A}} d \sum_{\substack{1\le a\le A\\ d\,|\,a}} 1 = \sum_{\substack{d\,|\,m\\ d\le A}} d \left\lfloor \frac{A}{d}\right\rfloor \le A\ \tau(m) \tag{14}$$

which implies (12) and (13) when $|b| \le \frac{1}{2}$. □

3.4. **Gauss sums.**

Lemma 8. *For all $(a,b,m) \in \mathbb{Z}^3$ with $m \ge 1$, we have*

$$\left|\sum_{n=0}^{m-1} \mathrm{e}\left(\tfrac{an^2+bn}{m}\right)\right| \le \sqrt{2m\gcd(a,m)}. \tag{15}$$

Proof. This is Proposition 2 of [9]. □

For incomplete quadratic Gauss sums we have

Lemma 9. *For all $(a,b,m,N,n_0) \in \mathbb{Z}^5$ with $m \ge 1$ and $N \ge 0$, we have*

$$\left|\sum_{n=n_0+1}^{n_0+N} \mathrm{e}\left(\tfrac{an^2+bn}{m}\right)\right| \le \left(\tfrac{N}{m} + 1 + \tfrac{2}{\pi}\log\tfrac{2m}{\pi}\right)\sqrt{2m\gcd(a,m)}. \tag{16}$$

Proof. The following argument is a variant of a method known at least since Vinogradov. For $m = 1$ the result is true. Assume that $m \ge 2$. 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 $1 \le L \le m$. 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

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

Applying Lemma 8 with b replaced by $b+k$ and observing (by convexity of $t \mapsto 1/\sin(\pi t/m)$) that

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

we obtain (16). □

3.5. **Norm of matrix products.**

Lemma 10. *Let $\mathbf{M}_\ell$, $\ell \in \mathbb{N}$, be $N \times N$-matrices with complex entries $M_{\ell;i,j}$, $1 \le i,j \le N$, and absolute row sums*

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

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

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

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

(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*

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

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

$$\left\| \prod_{\ell=r}^{r+k-1} \mathbf{M}_\ell \right\|_\infty \le C 2^{-\delta k} \tag{17}$$

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

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 (17) 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 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 10. □

4. Carry Lemmas

The first lemma is a reformulation of Lemma 16 of [9].

Lemma 11. *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*

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

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

The next lemma is more involved.

Lemma 12. *Let $(\lambda,\mu,\nu)\in\mathbb{N}^3$ such that $0<\mu<\nu<\lambda$ and set $\mu'=\mu-\rho'$, where ρ' is an integer satisfying $2\rho'\le\mu\le\nu-\rho'$ 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 set*

$$\begin{aligned}
n^2&\equiv u_1 2^{\mu'}+w_1 \bmod 2^\lambda && (0\le w_1<2^{\mu'},\ 0\le u_1<2^{\lambda-\mu+\rho'})\\
(n+r)^2&\equiv u_2 2^{\mu'}+w_2 \bmod 2^\lambda && (0\le w_2<2^{\mu'},\ 0\le u_2<2^{\lambda-\mu+\rho'})\\
2n&\equiv u_3 2^{\mu'}+w_3 \bmod 2^\lambda && (0\le w_3<2^{\mu'},\ 0\le u_3<2^{\nu+1-\mu+\rho'})\\
2sn&\equiv v \bmod 2^{\lambda-\mu}, && (0\le v<2^{\lambda-\mu})
\end{aligned}\tag{18}$$

where the integers $u_1=u_1(n)$, $u_2=u_2(n)$,$u_3=u_3(n)$, $v=v(n)$,$w_1=w_1(n)$, $w_2=w_2(n)$ and $w_3=w_3(n)$ satisfy the above conditions. Then for any integer $\ell\ge 1$ the number of integers $n<2^\nu$ for which one of the following conditions

$$\begin{aligned}
\mathrm{s}_{\mu,\lambda}((n+\ell)^2)&\ne\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3)\\
\mathrm{s}_{\mu,\lambda}((n+\ell+s2^\mu)^2))&\ne\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+v2^{\rho'}+\ell s2^{\rho'+1})\\
\mathrm{s}_{\mu,\lambda}((n+r+\ell)^2)&\ne\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3)\\
\mathrm{s}_{\mu,\lambda}((n+r+\ell+s2^\mu)^2))&\ne\mathrm{s}_{\rho',\lambda-\mu+\rho'}(u_2+\ell u_3+v2^{\rho'}+(\ell+r)s2^{\rho'+1})
\end{aligned}\tag{19}$$

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

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

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 (18), then we have

$$\frac{(n+\ell)^2}{2^\mu}-\left\lfloor\frac{(n+\ell)^2}{2^\mu}\right\rfloor\le\frac{C}{2^{\rho'}}\quad\text{or}\quad\frac{(n+\ell)^2}{2^\mu}-\left\lfloor\frac{(n+\ell)^2}{2^\mu}\right\rfloor\ge 1-\frac{C}{2^{\rho'}},\tag{20}$$

where $C = C(\ell)$ is a constant.

(2) The number of integers $n < 2^\nu$ with (20) is $\ll 2^{\nu-\rho'}$.

Of course if these two properties are true then Lemma 12 is proven.

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

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

is bounded and, thus, can only attain finitely many values $\{1, 2, \ldots, D\}$ (where D is a constant that depends on ℓ). 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 $0 \leq \tilde{v} < 2^{\rho'}$. Then the digits $\varepsilon_j(u_1 + \ell u_3)$, $\rho' \leq j < \lambda - \mu'$, might be affected by this carry if $\tilde{v} \in \{2^{\rho'} - 1, 2^{\rho'} - 2, \ldots, 2^{\rho'} - D\}$. 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 (20) holds with $C = D + 1$. This completes the proof of the first part.

Next let Z denote the number integers of $n < 2^\nu$ with (20). Then by Lemma 2 we have

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

where $\alpha = C2^{-\rho'}$ 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 $h \neq 0$ with $|h| \leq H = 2^{\rho'}$ can be written as $h = h'2^t$, where $0 \leq t \leq \rho'$ and h' is odd with $|h'| \leq 2^{\rho'-t}$. Then we have by Lemma 9

$$\sum_{n<2^\nu} \mathrm{e}\left(h\frac{(n+1)^2}{2^\mu}\right) = O\left(2^{\nu+(t-\mu)/2} + \mu 2^{(\mu+t)/2}\right)$$

and consequently

$$\begin{aligned}&2^{-\rho'} \sum_{0\neq|h|\leq 2^{\rho'}} \left|\sum_{n<2^\nu} \mathrm{e}\left(h\frac{(n+1)^2}{2^\mu}\right)\right|\\ &= O\left(2^{-\rho'} \sum_{0\leq t\leq\rho'} 2^{\rho'-t}\left(2^{\nu+(t-\mu)/2} + \mu 2^{(\mu+t)/2}\right)\right)\\ &= O\left(2^{\nu-\mu/2} + \mu 2^\mu\right).\end{aligned}$$

Since $2\rho' \leq \mu \leq \nu - \rho'$ 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 the term $s2^\mu$ does not affect the discussed carry propagation. Next for $(n + \ell + r)^2$ we have

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

Here we have to assure that $2^{-\mu'}(w_2 + \ell w_3 + \ell^2 + 2r\ell)$ remains bounded. However, this is ensured by the assumption $\lambda - \nu \leq 2(\mu - \rho')$. The same argument applies for the final case $(n+\ell+s2^\mu+r)^2$. □

5. 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 $(d, \lambda) \in \mathbb{N}^2$,

$$G_\lambda^I(h,d) = \frac{1}{2^\lambda} \sum_{0 \le u < 2^\lambda} \mathrm{e}\left(\sum_{\ell=0}^{k-1} \alpha_\ell f_\lambda(u + \ell d + i_\ell) - hu2^{-\lambda} \right), \tag{21}$$

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

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

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

$$G_\lambda^I(h, 2d+\varepsilon) = \frac{(-1)^{|I|+\sigma\varepsilon}}{2} G_{\lambda-1}^{T_{\varepsilon 0}(I)}(h,d) + \frac{(-1)^{|I|+K+\sigma\varepsilon}\,\mathrm{e}(-h/2^\lambda)}{2} G_{\lambda-1}^{T_{\varepsilon 1}(I)}(h,d). \tag{22}$$

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

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

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 8 and 9.

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.

6. 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

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

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

$$\mu < \nu < \lambda \text{ and } \lambda - \nu = \nu - \mu = \tfrac{1}{2}(\lambda - \mu) \tag{23}$$

(the precise values will be specified later).

By using Lemma 11 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 if follows that we obtain for those n

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

where $\mathrm{s}_{\lambda,\infty} = \mathrm{s} - \mathrm{s}_\lambda$. Consequently, if we set

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

then

$$S_0 = S_1 + O\left(2^{\nu-(\lambda-\nu)}\right). \tag{24}$$

Next we apply Lemma 5 with $Q = 2^\mu$ and $S = 2^{\nu-\mu}$ and obtain

$$|S_1|^2 \ll \frac{N^2}{S} + \frac{N}{S}\Re(S_2), \tag{25}$$

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 $\rho' > 0$ will be chosen in a proper way. We set

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

where the integers $u_1 = u_1(n)$, $u_3 = u_3(n)$, $v = v(n)$, $w_1 = w_1(n)$, and $w_3 = w_3(n)$ satisfy the above conditions. Then, by assuming that

$$2\mu' \ge \lambda, \tag{26}$$

we have

$$\begin{aligned} (n+\ell)^2 &\equiv (u_1 + \ell u_3)2^{\mu'} + w_1 + \ell w_3 + \ell^2 \bmod 2^\lambda, \\ (n+\ell+s2^\mu)^2 &\equiv (u_1 + \ell u_3 + v2^{\rho'} + \ell s 2^{\rho'+1})2^{\mu'} + w_1 + \ell w_3 + \ell^2 \bmod 2^\lambda. \end{aligned}$$

By Lemma 12 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

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

where $u_1 = u_1(n), u_3 = u_3(n), v = v(n)$, since we certainly have

$$S_2'(s) = S_3'(s) + O(2^{\nu-\rho'}). \tag{27}$$

Next we rewrite $S_3'(s)$ as

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

where χ_α is defined by (2). Lemma 3 allows us to replace the product of characteristic functions χ by a product of trigonometric polynomials. More precisely, using (8) 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

$$S_3'(s) = S_4(s) + O(E_1) + O(E_3) + O(E_{1,3}), \tag{28}$$

with

$$\begin{aligned} S_4(s) \;=\; & \sum_{0\le u_1<U_1}\sum_{0\le u_3<U_3}\sum_{0\le v<2^{\lambda-\mu}} \\ & \sum_{n\in I(N,s)} \mathrm{e}\left(\sum_{\ell=0}^{k-1}\alpha_\ell(f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3)-f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+v(n)2^{\rho'}+\ell s2^{\rho'+1})\right) \\ & A_{U_1^{-1},H_1}\left(\frac{n^2}{2^\lambda}-\frac{u_1}{U_1}\right)A_{U_3^{-1},H_3}\left(\frac{2n}{2^{\nu+1}}-\frac{u_3}{U_3}\right)\frac{1}{2^{\lambda-\mu}}\sum_{0\le h<2^{\lambda-\mu}}\mathrm{e}\left(h\frac{2sn-v}{2^{\lambda-\mu}}\right), \end{aligned}$$

where we have *filtered* the correct value of $v=v(n)$ and where the error terms E_1, E_3, $E_{1,3}$ can be easily estimated with the help of Lemma 9 (and obvious estimates):

$$E_1=\frac{1}{2^{\rho''}}\sum_{|\overline{h}_1|\le 2^{\rho''}}\left|\sum_n \mathrm{e}\left(\frac{\overline{h}_1n^2}{2^{\mu'}}\right)\right|\ll 2^{\nu-\rho''}+\rho''2^{\nu-\mu'/2}\ll 2^{\nu-\rho''},$$

$$E_3=\frac{1}{2^{\rho''}}\sum_{|\overline{h}_3|\le 2^{\rho''}}\left|\sum_n \mathrm{e}\left(\frac{\overline{h}_32n}{2^{\mu'}}\right)\right|\ll 2^{\nu-\rho''}+\rho''2^{\nu-\mu'}\ll 2^{\nu-\rho''},$$

$$E_{1,3}=\frac{1}{2^{2\rho''}}\sum_{|\overline{h}_1|\le 2^{\rho''}}\sum_{|\overline{h}_3|\le 2^{\rho''}}\left|\sum_n \mathrm{e}\left(\frac{\overline{h}_1n^2}{2^{\mu'}}+\frac{\overline{h}_32n}{2^{\mu'}}\right)\right|\ll 2^{\nu-\rho''},$$

provided that

$$\rho''<\mu'/2 \text{ and } \mu'\ll 2^{\nu-\mu'}. \tag{29}$$

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 $S_4(s)$. By using the representation of $A_{U_1^{-1},H_1}$ and $A_{U_3^{-1},H_3}$ we obtain

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

where by (5),

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

The first step in the analysis of the main term of $S_4(s)$ is to observe that we only have to take into accout 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 9 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

$$\sum_{1\le h_1\le H_1}\sqrt{\gcd(h_1,2^\lambda)}\le\sum_{0\le i\le\lambda}2^{i/2}\sum_{\substack{1\le h_1\le H_1\\ 2^i\mid h_1}}1=\sum_{0\le i\le\lambda}2^{i/2}\left\lfloor\frac{H_1}{2^i}\right\rfloor\le\frac{H_1}{1-2^{-1/2}},\tag{30}$$

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

$$(\nu-\mu)+2(\lambda-\mu)+2(\rho'+\rho'')\le\lambda/4\tag{31}$$

(which will be justified later) so that

$$S_4(s)=S_5(s)+O(\lambda 2^{3\lambda/4}),\tag{32}$$

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

$$\begin{aligned}|S_5(s)|\le\frac{1}{U_1U_32^{\lambda-\mu}}\sum_{|h_3|\le H_3}\sum_{0\le h<2^{\lambda-\mu}}\sum_{0\le u_3<U_3}\\ \left|\sum_{0\le u_1<U_1}\sum_{0\le v<2^{\lambda-\mu}}\mathrm{e}\left(\sum_{\ell=0}^{k-1}\alpha_\ell(f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3)-f_{\rho',\lambda-\mu+\rho'}(u_1+\ell u_3+v2^{\rho'}+\ell s2^{\rho'+1}))-\frac{hv}{2^{\lambda-\mu}}\right)\right|\\ \times\min\left(N,\left|\sin\left(\pi\left(\frac{h_3}{2^\nu}+\frac{2hs}{2^{\lambda-\mu}}\right)\right)\right|^{-1}\right).\end{aligned}$$

By 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 $\mathcal{I}_k$, we have

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

By substituting $u_1'+v$ by another variable $\overline{u}_1'$, by using the definition of $G^I_{\lambda-\mu}(h,d)$ 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 (23)) 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. Since $|h_3|/2^\nu\le 1/2$ we obtain from (13)

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

Finally we have

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

and thus we obtain the estimate

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

provided that

$$\nu-\mu'+\rho''+\lambda-\mu\le\nu. \tag{33}$$

Putting all these estimates together (and recalling that $\mu'=\mu-\rho'$), from (24), (25), (27), (28), (32) we finally get the upper bound

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

provided that the conditions (23) (26), (29), (31), (33) hold:

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

For example the choice

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

ensures that the above conditions are satisfied.

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.

7. 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

$$0 \le \rho_1 < \rho < \mu = \nu - 2\rho < \nu < \lambda = \nu + 2\rho < 2\nu \tag{34}$$

to be chosen later. We apply Lemma 5 with $Q = 1$ and $R = 2^\rho$, we sum trivially for $1 \le r \le R_1 = 2^{\rho_1}$ and obtain

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

where

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

and $I_1(r)$ is an interval included in $[0, N-1]$. By Lemma 11 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 such that $1 \le \rho' \le \rho$. Applying Lemma 5 with $Q = 2^\mu$ and

$$S = 2^{2\rho'} \le 2^{\nu-\mu}, \tag{35}$$

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

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

we get

$$|S_0|^4 \ll 2^{4\nu-2\rho+2\rho_1} + 2^{6\nu+2\rho-2\lambda} + \frac{2^{4\nu}}{S} + \frac{2^{3\nu}}{RS} \sum_{R_1<r<R} \sum_{1\le s<S} |S_2(r,s)|, \tag{36}$$

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 $\mu' = \mu - \rho' > 0$. Writing

$$U = 2^{\lambda-\mu+\rho'},\ U_3 = 2^{\nu-\mu+\rho'+1}, V = 2^{\lambda-\mu}, \tag{37}$$

we assume that

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

where the integers $u_1 = u_1(n)$, $u_2 = u_2(n)$, $u_3 = u_3(n)$, $v = v(n)$, $w_1 = w_1(n)$, $w_2 = w_2(n)$, and $w_3 = w_3(n)$ verify the above conditions. Assuming that $\lambda \le 2\mu'$, we have

$$\begin{aligned}
(n+\ell)^2 &\equiv (u_1 + \ell u_3)2^{\mu'} + w_1 + \ell w_3 + \ell^2 \bmod 2^\lambda,\\
(n+\ell+s2^\mu)^2 &\equiv (u_1 + \ell u_3 + v2^{\rho'} + \ell s 2^{\rho'+1})2^{\mu'} + w_1 + \ell w_3 + \ell^2 \bmod 2^\lambda,\\
(n+\ell+r)^2 &\equiv (u_2 + \ell u_3)2^{\mu'} + w_2 + \ell w_3 + \ell^2 + 2r\ell \bmod 2^\lambda,\\
(n+\ell+s2^\mu+r)^2 &\equiv (u_2 + \ell u_3 + v2^{\rho'} + (\ell+r) s 2^{\rho'+1})2^{\mu'} + w_2 + \ell w_3 + \ell^2 + 2r\ell \bmod 2^\lambda.
\end{aligned}$$

According to Lemma 12, uniformly for fixed integers $r, s, \ell \ge 1$, the number of integers $n < 2^\nu$ for which at least one of the following conditions

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

is satisfied is $\ll 2^{\nu-\rho'}$. Filtering now by the values of u_1, u_2, u_3, it follows that

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

Lemma 3 allows us to replace the product of characteristic functions χ by a product of trigonometric polynomials. More precisely, using (8) $U_1 = U_2 = U$, $H_1 = H_2 = U2^{\rho_2}$ and $H_3 = U_3 2^{\rho_3}$, where the integers ρ_2 and ρ_3 verify

$$\rho_2 \le \mu - \rho',\ \rho_3 \le \mu - \rho', \tag{38}$$

we obtain

$$S_2(r,s) = S_3(r,s) + O(2^{\nu-\rho'}) + O\left(E_{30}(r)\right) + O\left(E_{31}(0)\right) + O\left(E_{31}(r)\right) + O\left(E_{32}(0)\right) + O\left(E_{32}(r)\right) + O\left(E_{33}(r)\right) + O\left(E_{34}(r)\right), \tag{39}$$

with

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

We have

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

which by (12) and (37) gives

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

Similarly we have

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

which gives by (15) (for which we have $2^{\nu-\mu+\rho'}$ complete sums), (30) and (38)

$$\begin{aligned} E_{31}(r) &\ll 2^{\nu-\rho_2} + 2^{-\rho_2}\sum_{1\le h_2'\le 2^{\rho_2}} 2^{\nu-\mu+\rho'}\sqrt{\gcd(h_2',2^{\mu-\rho'})} \\ &\ll 2^{\nu-\rho_2} + 2^{\nu-\mu+\rho'} \le 2^{\nu-\rho_2}. \end{aligned}$$

Similarly we have

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

which gives by (15), (30) and (38), with a trivial summation over h_3',

$$E_{32}(r) \ll 2^{\nu-\rho_2} + 2^{-\rho_2}\sum_{1\le h_2'\le 2^{\rho_2}} 2^{\nu-\mu+\rho'}\sqrt{\gcd(h_2',2^{\mu-\rho'})} \ll 2^{\nu-\rho_2}.$$

Similarly again we have

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

which gives by (15), (30) and (38), writing $h'=h_1'+h_2'$,

$$E_{33}(r)\ll 2^{\nu-\rho_2}+2^{-\rho_2}\sum_{1\le h'\le 2^{\rho_2+1}}2^{\nu-\mu+\rho'}\sqrt{\gcd(h',2^{\mu-\rho'})}\ll 2^{\nu-\rho_2}.$$

Similarly once more we have

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

which gives by (15), (30) and (38), writing $h'=h_1'+h_2'$, with a trivial summation over h_3',

$$E_{34}(r)\ \ll\ 2^{\nu-\rho_2}+2^{-\rho_2}\sum_{1\le h'\le 2^{\rho_2+1}}2^{\nu-\mu+\rho'}\sqrt{\gcd(h',2^{\mu-\rho'})}\ll 2^{\nu-\rho_2}.$$

We deduce from (39) that

$$S_2(r,s)=S_3(r,s)+O(2^{\nu-\rho'})+O(2^{\nu-\rho_2})+O(2^{\nu-\rho_3}) \tag{40}$$

and we can write

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

Let us introduce the decomposition

$$S_3(r,s)=S_4(r,s)+S_4'(r,s), \tag{41}$$

where $S_4(r,s)$ denotes the contribution of the terms for which $h_1+h_2=0$ while $S_4'(r,s)$ denotes the contribution of the terms for which $h_1+h_2\ne 0$. We have by (16)

$$\begin{aligned}S_4'(r,s)\ &\ll\ \sum_{|h_1|\le H_1}a_{h_1}(U^{-1},H_1)\sum_{|h_2|\le H_2}a_{h_2}(U^{-1},H_2)\sum_{|h_3|\le H_3}a_{h_3}(U_3^{-1},H_3)\\
&\qquad U^2U_3V\lambda 2^{\lambda/2}\sqrt{\gcd(h_1+h_2,2^\lambda)}\\
&\ll\ \nu^3U^2U_3V\lambda 2^{\lambda/2}\sqrt{2H_2}\\
&\ll\ \nu^4 2^{\nu+\frac12(8\lambda-9\mu+7\rho'+\rho_2)},\end{aligned}$$

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

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

Using (21) 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

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

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

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

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

$$S_6(h_2,s,u'',u_3'') = \sum_{0\le u_3'<U_3'} \sum_{0\le h'<2^{\lambda-\mu}} \left|G_{\lambda-\mu}^{I(u'',u_3'')}(h'-h_2,u_3')\right|^2 \left|G_{\lambda-\mu}^{I(u'',u_3'')}(h',u_3'+2s)\right|^2. \tag{42}$$

We obtain

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

Observing that

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

we have by (11)

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

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

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

We recall here that in (36) we have $R_1 < r < R$ and introduce the integers H_2' and κ such that

$$H_2' = 2^{\lambda-\nu+1}H_3/R_1 = 2^{\lambda-\mu+\rho'+\rho_3-\rho_1+2} = 2^\kappa. \tag{43}$$

By (37), assuming that

$$\rho' + \rho_3 + 2 < \rho_1, \tag{44}$$

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

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

where $S_{41}(r,s)$, $S_{42}(r,s)$ and $S_{43}(r,s)$ denote respectively the contribution above of the terms $|h_2| \le H_2'$, $H_2' < |h_2| \le 2^{\lambda-\mu}$, $2^{\lambda-\mu} < |h_2| \le H_2$.

7.1. **Estimate of $S_{41}(r,s)$.** By (11) we have

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

so that

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

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'':

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

It follows from (42) 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

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

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 (43), (37) and (14)

$$\frac{1}{RS}\sum_{R_1<r<R}\sum_{1\le s<S} S_{41}(r,s) \ll \nu\,(\lambda-\mu)^2\ 2^{\nu-\eta'(\rho_1-\rho'-\rho_3)}. \tag{45}$$

7.2. **Estimate of $S_{42}(r,s)$.** The condition $|h_2|>H_2'$ ensures that $2^{\lambda-\nu}|h_3|\le\frac12|h_2r|$ so that

$$\min\left(2^\nu,\left|\sin\pi\tfrac{h_2r+2^{\lambda-\nu}h_3}{2^{\lambda-1}}\right|^{-1}\right)\ll\frac{2^\lambda}{H_2'r}.$$

By the Cauchy-Schwarz inequality we have

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

It follows that

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

and we get by (43) and (37),

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

so that by (14)

$$\frac{1}{RS}\sum_{R_1<r<R}\sum_{1\le s<S}S_{42}(r,s) \ll \rho(\lambda-\mu)^3\ 2^{\nu-\rho+\rho_1+\rho'-\rho_3}. \tag{46}$$

7.3. **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 $|h_2| > j2^{\lambda-\mu}$ ensures that $2^{\lambda-\nu}|h_3| \le \frac12|h_2r|$ so that

$$\min\left(2^\nu, \left|\sin\pi\tfrac{h_2r+2^{\lambda-\nu}h_3}{2^{\lambda-1}}\right|^{-1}\right) \ll \frac{2^\lambda}{j2^{\lambda-\mu}r} = \frac{2^\mu}{jr}.$$

By the Cauchy-Schwarz inequality we have

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

It follows that

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

so that by (37) and (14)

$$\frac{1}{RS}\sum_{R_1<r<R}\sum_{1\le s<S}S_{43}(r,s) \ll \rho\ (\lambda-\mu)^3\ 2^{\nu-\rho+3\rho'}. \tag{47}$$

It follows from (45), (46) and (47) that

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

Choosing

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

we obtain

$$\frac{1}{RS}\sum_{R_1<r<R}\sum_{1\le s<S}S_4(r,s) \ll \nu^4 2^\nu\left(2^{-\eta'(\rho-3\rho')}+2^{-\rho'}+2^{-(\rho-3\rho')}\right). \tag{48}$$

Using (41) and (40), since $0<\eta'<1$ we obtain

$$\frac{1}{RS}\sum_{R_1<r<R}\sum_{1\le s<S}S_2(r,s) \ll \nu^4 2^\nu\left(2^{-\eta'(\rho-3\rho')}+2^{-\rho'}+2^{\frac12(8\lambda-9\mu+8\rho')}\right) \tag{49}$$

that we can insert in (36), recalling by (35) that $S = 2^{2\rho'}$ and by (34) that $\mu = \nu - 2\rho$, $\lambda = \nu + 2\rho$, so that we get

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

and if we set $\rho' = \lfloor \nu/146 \rfloor$ and $\rho = 4\rho'$ we obtain

$$|S_0| \ll \nu 2^{\nu - \frac{\eta'\rho'}{4}} \ll \nu N^{1-\eta''} \tag{50}$$

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

8. Proof of Proposition 1

8.1. **Proof of Proposition 1 in the case** $(\alpha_0, \dots, \alpha_{k-1}) = (1, \dots, 1)$**.** With the help of Lemma 13 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

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

If we split up the sum over $0 \le d < 2^{\lambda'}$ into even and odd d, this gives rise to a vector recurrence for $\boldsymbol{\psi}_{\lambda,\lambda'}(h) = \left(\Phi_{\lambda,\lambda'}^{I,I'}(h)\right)_{(I,I')\in\mathcal{I}_k^2}$ 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, λ' and $\beta = h/2^\lambda$. By construction all absolute row sums of $\mathbf{M}(\beta)$ are equal to 1. More precisely in each row there are eight non-zero entries, where all of them are either equal to $\pm 1/8$ or equal to $\pm\,\mathrm{e}(\pm\beta)/8$.

It is convenient to interpret these matrices as weighted directed graphs, where the vertices are the pairs $(I, I') \in \mathcal{I}_k^2$ and starting from each vertex there are 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. Of course products of m such matrices correspond to

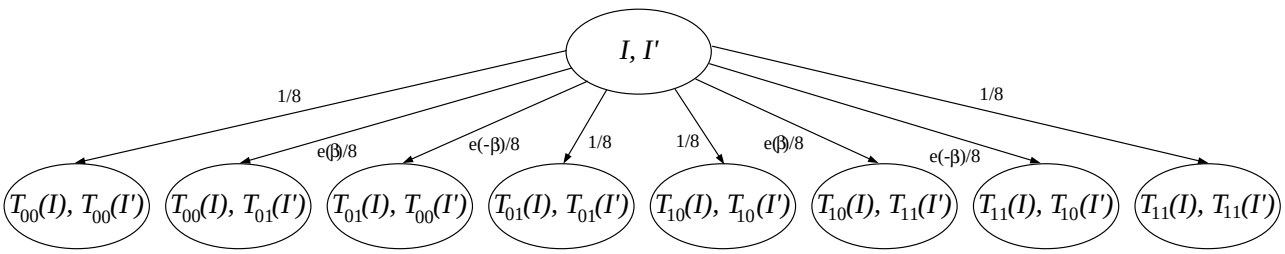


Figure 1. Weighted directed graph representation of the recurrence for $\Phi_{\lambda,\lambda'}^{I,I'}(h)$ (the common sign of all the edge weights is $(-1)^{|I|+|I'|}$).

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 10 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 (17) with $k=\lambda'$ and $r=\lambda-\lambda'+1$ that

$$\|\boldsymbol{\psi}_{\lambda,\lambda'}(h)\|_\infty \le C2^{-\delta\lambda'}\,\|\boldsymbol{\psi}_{\lambda-\lambda',0}(h)\|_\infty \le C2^{-\delta\lambda'} \ll 2^{-\delta\lambda/2} \tag{51}$$

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 $\mathbf{A} = (A_{(I,I'),(J,J')})_{((I,I'),(J,J'))\in\mathcal{I}_k^2\times\mathcal{I}_k^2}$ of m_0 consecutive matrices $\mathbf{M}_\ell = \mathbf{M}(h/2^\ell)$ verifies the condition (1) of Lemma 10. 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 $> 1-8^{-m_0}/2$.

Finally we show that there exists an integer $m_1\ge 1$ such that every product $\mathbf{B} = (B_{(I,I'),(J,J')})_{((I,I'),(J,J'))\in\mathcal{I}_k^2\times\mathcal{I}}$ of m_1 consecutive matrices $\mathbf{M}_\ell = \mathbf{M}(h/2^\ell)$ verifies the condition (2) of Lemma 10. 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 just 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 $011\cdots 1$, 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 one time the transformation (T_{01},T_{01}), then m_1-3 times 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 10 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.

8.2. **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 8.1 that the conditions of Lemma 10 are satisfied.

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

9. Proof of Proposition 2

9.1. **Proof of Proposition 2 in the case** $(\alpha_0,\dots,\alpha_{k-1}) = (1,\dots 1)$**.** Formula (22) 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

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

By Lemma 10, Proposition 2 will follow from the fact that there exists an integer $m \geq 1$ such that for any $\mathbf{d} \in \{0,1\}^m$ and $I \in \mathcal{I}_k$,

$$\max_{z \in \mathbb{U}} \sum_{J \in \mathcal{I}_k} \left| P_{IJ}^{\mathbf{d}}(z) \right| < 2^m.$$

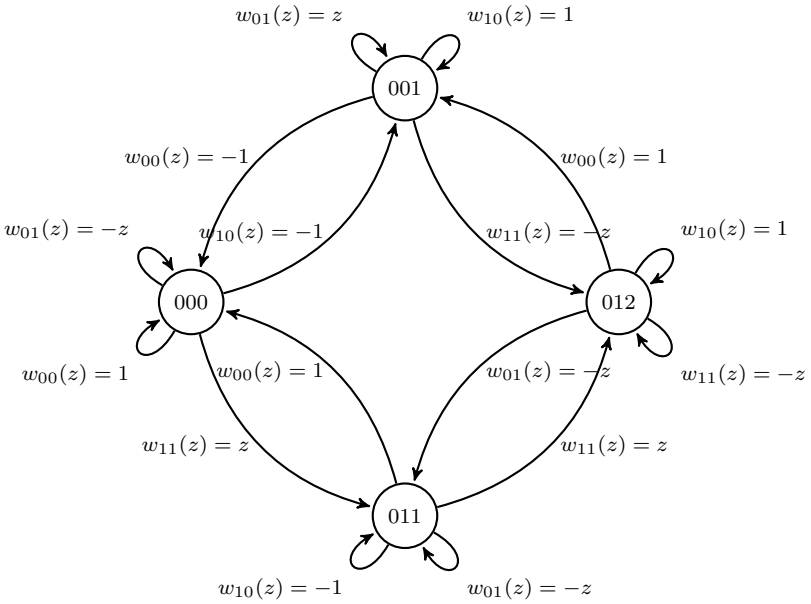
The end of this section is devoted to a proof of this fact.

Let $\mathcal{G}(z)$ be the weighted directed 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 $T_i^{\mathbf{de}}(I) = T_{d_{i-1}e_{i-1}} \circ \cdots \circ T_{d_0e_0}(I)$ and associate to each of the 2^m paths from the vertex I to the vertices $T_m^{\mathbf{de}}(I)$ 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

$$\nu(I,\mathbf{d},\mathbf{e}) = |I| + \left|T_1^{\mathbf{de}}(I)\right| + \cdots + \left|T_{m-1}^{\mathbf{de}}(I)\right| + |\mathbf{d}|\,\sigma + |\mathbf{e}| \tag{52}$$

and

$$N(\mathbf{e}) = \sum_{i=0}^{m-1} e_i 2^i. \tag{53}$$

Then, for any $(I,J)\in\mathcal{I}_k^2$, we have, by definition of $P_{IJ}^{\mathbf{d}}$:

$$P_{IJ}^{\mathbf{d}}(z)=\sum_{\substack{\mathbf{e}\in\{0,1\}^m\\ T_m^{\mathbf{de}}(I)=J}} w^{\mathbf{de}}(I,z)=\sum_{\substack{\mathbf{e}\in\{0,1\}^m\\ T_m^{\mathbf{de}}(I)=J}}(-1)^{\nu(I,\mathbf{d},\mathbf{e})}z^{N(\mathbf{e})}. \tag{54}$$

Lemma 14. *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 (54) that (1) is a direct consequence of the fact that the function N defined by (53) is a bijection between $\{0,1\}^m$ and $\{0,\dots,2^{m-1}\}$ and (2) of the fact that for any $J\in\mathcal{I}_k$, 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 15. *Let $(I_0,I_1)\in\mathcal{I}_k^2$ and $j\in\{0,\dots,k-1\}$ such that $I_{0|j}-I_{1|j}\in\{0,1\}$. 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 15 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 16. *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 $I_{e_0}=T_{d_0e_0}(I)$.

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 16 is true in these two cases with $m=1$.

In any other case, we have $I_0\ne I_1$ 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

$$T_{d_{m-1}e_{m-1}}\circ\cdots\circ T_{d_1e_1}(I_0)=T_{d_{m-1}e_{m-1}}\circ\cdots\circ T_{d_1e_1}(I_1).$$

Let j_1 be the smallest integer j such that $I_{0|j}=I_{1|j}+1$ and choose, by Lemma 15, $e_1\in\{0,1\}$ such that $T_{d_1e_1}(I_0)_{|j_1}=T_{d_1e_1}(I_1)_{|j_1}+0$. By repeating this procedure $m-1\le k-1$ 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 16. □

Lemma 16 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 $\pm z^{N(\mathbf{e})+1}$. The end of the proof of Proposition 2 is based on Lemma 17 which will be deduced from Lemma 18 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 17. *For any $\mathbf{d} \in \{0,1\}^{k+1}$ and any $I \in \mathcal{I}_k$ we have*

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

Proof. Lemma 16 implies 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 $z \in \{-1, +1\}$. Moreover, for any $\varepsilon \in \{0,1\}$, it follows from the relation

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

(we put $\mathbf{d}' = (\varepsilon, d_0, \dots, d_{k-1})$ and we consider the coefficients (I, J) of the matrix $\mathbf{M}^{\mathbf{d}'}(z) = \mathbf{M}^{\varepsilon}(z)\mathbf{M}^{\mathbf{d}}(z^2)$) that if, for any $I \in \mathcal{I}_k$ we have $\sum_{J \in \mathcal{I}_k} \left| P_{IJ}^{\mathbf{d}}(1) \right| < 2^k$ then for any $I \in \mathcal{I}_k$, we have $\sum_{J \in \mathcal{I}_k} \left| P_{IJ}^{\mathbf{d}'}(-1) \right| < 2^{k+1}$. It follows that in order to prove Lemma 17 it is enough to prove that for any $d \in \{0,1\}^k$ and any $I \in \mathcal{I}_k$, we have $\sum_{J \in \mathcal{I}_k} \left| P_{IJ}^{\mathbf{d}}(1) \right| < 2^k$. This will be an immediate consequence of Lemma 18 below. □

Lemma 18. *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-uples $I_0(\ell) = T_{d_{\ell-1}e_{\ell-1}} \circ \cdots \circ T_{d_1 e_1}(I_0)$ 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 16. 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 18 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 16 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 on 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 $(T_{d_{\ell_0}0}(I_0(\ell)),\ T_{d_{\ell_0}0}(I_1(\ell)))$ and $(T_{d_{\ell_0}1}(I_0(\ell)),\ T_{d_{\ell_0}1}(I_1(\ell)))$, which are the possible candidates for $(I_0(\ell_0+1), I_1(\ell_0+1))$ it follows

from Lemma 15 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 $T_{d_{\ell_0}0}(I_0(\ell))$ and $T_{d_{\ell_0}0}(I_1(\ell))$ or $T_{d_{\ell_0}1}(I_0(\ell))$ and $T_{d_{\ell_0}1}(I_1(\ell))$ differ at an odd number of positions (and the other one at an even number of positions). Suppose without loss of generality that $T_{d_{\ell_0}0}(I_0(\ell))$, $T_{d_{\ell_0}0}(I_1(\ell))$ differs by an odd number of positions. If $T_{d_{\ell_0}1}(I_0(\ell)) = T_{d_{\ell_0}1}(I_1(\ell))$ then we choose $e_{\ell_0+1} = 1$ and the procedure stops. However, if $T_{d_{\ell_0+1}1}(I_0(\ell)) \neq T_{d_{\ell_0+1}1}(I_1(\ell))$ then we choose $e_{\ell_0+1} = 0$ 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 $T_{d_{m_0}\widetilde{e}_{m_0}}(I_0(m_0)) = I_0(m_0)$ and $T_{d_{m_0}\widetilde{e}_{m_0}}(I_1(m_0)) = I_1(m_0)$ (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 $I_0(m_0) = I_0(m_0+1)$ and $I_1(m_0) = I_1(m_0+1)$ (and of course they differ at an 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

$$\nu(I, \mathbf{d}, \mathbf{e}) \equiv \nu(I, \mathbf{d}, \mathbf{e}') + (m_0 + 1 - \ell_0 + 1) + 1 \bmod 2 \equiv \nu(I, \mathbf{d}, \mathbf{e}') + 1 \bmod 2 \tag{55}$$

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 (55) 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. □

9.2. **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 $\ell \ge 1$ we have $\alpha_\ell = 0$. As we mentionned in Section 8.2, 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 $\tilde{I} = (i_\ell)_{0 \le \ell < k,\, \alpha_\ell = 1}$ 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 $m \ge 1$, $\mathbf{d} \in \{0,1\}^m$ 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 14. 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 $\widetilde{P}_{\widetilde{I}\widetilde{J}}^{\mathbf{d}}$:

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

Next, the Lemmas 15, 16, and 18 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 16, and 18 directly translate to this case. For example we can project the two paths from the proof of Lemma 16 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 $\widetilde{P}_{\widetilde{I}\widetilde{J}}^{\mathbf{d}}$ contains two monomials of consecutive degrees and then show, as in Lemma 18, that we can find $\widetilde{J} \in \widetilde{\mathcal{I}}_k$ such that the polynomial $\widetilde{P}_{\widetilde{I}\widetilde{J}}^{\mathbf{d}}$ 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.

10. Conclusion, open problems

This work shows that it is possible, starting from an almost periodic sequence, to obtain a normal subsequence just by extracting along the squares. Our proof works (with some extra technicity) for any quadratic polynomial taking values in $\mathbb{N}$, but the two following problems are open.

Problem 1. *For any polynomial of degree at least* 3 *taking values in* $\mathbb{N}$*, is it true that* $(t(P(n)))_{n\in\mathbb{N}}$ *is normal ?*

Problem 2. *Let* $(p_n)_{n\in\mathbb{N}}$ *denote the sequence of prime numbers. For any non constant polynomial taking values in* $\mathbb{N}$*, is it true that* $(t(P(p_n)))_{n\in\mathbb{N}}$ *is normal ?* [1]

Moreover it would be interesting to find some other almost periodic sequences $\mathbf{u}$ with the same property and also to understand this phenomenon from the dynamical system point of view.

References

[1] J.-P. Allouche and J. Shallit, *The ubiquitous Prouhet-Thue-Morse sequence*, in Sequences and their applications (Singapore, 1998), Springer Ser. Discrete Math. Theor. Comput. Sci., Springer, London, 1999, pp. 1–16.

[2] ——, *Automatic sequences*, Cambridge University Press, Cambridge, 2003. Theory, applications, generalizations.

[3] 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.

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

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

[6] 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.

[7] P. Kůrka, *Topological and symbolic dynamics.*, Paris: Société Mathématique de France, 2003.

[1] Mauduit and Rivat proved in [10] that the frequencies of 0 and 1 in the sequence $(t(p_n))_{n\in\mathbb{N}}$ are equal to $\frac{1}{2}$.

[8] C. Mauduit, *Multiplicative properties of the Thue-Morse sequence*, Period. Math. Hungar., 43 (2001), pp. 137–153.
[9] C. Mauduit and J. Rivat, *La somme des chiffres des carrés*, Acta Mathematica, 203 (2009), pp. 107–148.
[10] ——, *Sur un problème de Gelfond: la somme des chiffres des nombres premiers*, Annals of Mathematics, 171 (2010), pp. 1591–1646.
[11] ——, *Prime numbers along Rudin–Shapiro sequences*, J. Eur. Math. Soc., (to appear).
[12] H. M. Morse, *Recurrent geodesics on a surface of negative curvature*, Trans. Amer. Math. Soc., 22 (1921), pp. 84–100.
[13] Y. Moshe, *On the subword complexity of Thue-Morse polynomial extractions*, Theoret. Comput. Sci., 389 (2007), pp. 318–329.
[14] E. Prouhet, *Mémoire sur quelques relations entre les puissances des nombres*, C. R. Acad. Sc. Paris, 33 (1851), p. 225.
[15] 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.
[16] M. Queffelec, *Substitution Dynamical Systems – Spectral Analysis*, vol. 1294 of Lecture Notes in Math., Springer Verlag, New-York – Berlin, 1987.
[17] A. Thue, *Über die gegenseitige Lage gleicher Teile gewisser Zeichenreihen.* Kristiania: J. Dybwad. 67 S. Lex. 8° (1912)., 1912.
[18] J. Vaaler, *Some extremal functions in Fourier analysis*, Bull. Amer. Math. Soc., 12 (1985), pp. 183–216.

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

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

Institut de Mathématiques de Luminy, CNRS, Université d'Aix-Marseille, Campus de Luminy, Case 907, 13288 MARSEILLE Cedex 9, France