TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 370, Number 11, November 2018, Pages 7899–7921
http://dx.doi.org/10.1090/tran/7210
Article electronically published on May 9, 2018

RUDIN–SHAPIRO SEQUENCES ALONG SQUARES

CHRISTIAN MAUDUIT AND JOËL RIVAT

Abstract. We estimate exponential sums of the form $\sum_{n\le x} f(n^2)\mathrm{e}(\vartheta n)$ for a large class of digital functions f and $\vartheta \in \mathbb{R}$. We deduce from these estimates the distribution along squares of this class of digital functions which includes the Rudin–Shapiro sequence and some of its generalizations.

1. Introduction

For $x \in \mathbb{R}$, we denote by $\|x\|$ the distance of x to the nearest integer, and we set $\mathrm{e}(x) = \exp(2i\pi x)$. We denote by $\mathbb{U}$ the set of complex numbers of modulus 1. If f and g are two functions taking strictly positive values such that f/g is bounded, we write $f = O(g)$ or $f \ll g$. For $n \in \mathbb{N}$, we denote by $\tau(n)$ the number of divisors of n and by $\omega(n)$ the number of distinct prime factors of n. Throughout this work we denote by q an integer greater or equal to 2. Any $n \in \mathbb{N}$ can be written in base q as $n = \sum_{j\ge 0} \varepsilon_j(n) q^j$ with $\varepsilon_j(n) \in \{0, \dots, q-1\}$ for any $j \in \mathbb{N}$. If $\ell = \max\{j : \varepsilon_j(n) \neq 0\}$, we denote by $\mathrm{rep}_q(n) = \varepsilon_\ell(n) \cdots \varepsilon_0(n)$ the q-adic representation of the integer n.

1.1. **Representation of squares in base q.** There exists no simple algorithm to decide whether an integer is a square or not given its representation in base q. It follows from the work of Büchi concerning second-order weak arithmetic that the set of squares cannot be recognizable by a finite automaton (see [12]). Ritchie gave in [39] a very elegant proof of this result in the case of base $q = 2$, and Minsky and Papert showed in [33] the nonrecognizability of any zero density sequence of integers $(u_n)_{n\in\mathbb{N}}$ such that $\lim_{n\to\infty} u_{n+1}/u_n = 1$ (see also [14]). These facts explain why only a few results are known concerning the q-adic representation of squares or powers. Davenport and Erdős showed in [16] the normality of the real number whose q-adic representation is $0.\,\mathrm{rep}_q(P(1)) \cdots \mathrm{rep}_q(P(n)) \cdots$ when P is an integer valued polynomial. When s_q is the sum-of-digits function in base q, and d is an integer, where $d \ge 2$, Peter gave in [35] very precise informations about the behavior of $\sum_{n\le x} \mathrm{s}_q(n^d)$, and Bassily and Kátai studied in [4] the limit distribution of the sum-of-digits function along polynomial sequences.

Many important works concern the study of subsequences along squares or along integer valued polynomials since the questions asked by Bellow [5] and Furstenberg [21] and the proof by Bourgain in [7–9] of a pointwise ergodic theorem (see also in particular [6], [13], [22], [23]). We introduced in [29] a new method which gives

Received by the editors December 3, 2015, and, in revised form, February 16, 2017.
2010 *Mathematics Subject Classification.* Primary 11A63, 11B85, 11J71, 37A45.
Key words and phrases. Rudin–Shapiro sequences, exponential sums.
This work was supported by the Agence Nationale de la Recherche project ANR-14-CE34-0009 MUDERA and Ciência sem Fronteiras, projet PVE 407308/2013-0.

upper bounds for the exponential sums $\sum_{n\leq x} \mathrm{e}(\mathrm{s}_q(n^2)\alpha)$ (see [18] for a generalization to a larger class of digital sequences and [17] for higher-degree polynomials and large enough base q). One of the main ingredients of this method is to establish that the L^1-norm of the discrete Fourier transform of the sequence $(\mathrm{e}(\mathrm{s}_q(n)\alpha))_{n\in\mathbb{N}}$ is very small. Unfortunately, this property is generally not true for other digital sequences and, in particular, for Rudin–Shapiro sequences, and the goal of this paper is to present another method to study exponential sums associated to digital sequences.

1.2. **Rudin–Shapiro sequences and dynamical systems.** For any sequence $(r_n)_{n\in\mathbb{N}}$ in $\{-1,+1\}^{\mathbb{N}}$ we have

$$\sup_{\vartheta\in[0,1]} \left|\sum_{n<N} r_n \,\mathrm{e}(n\vartheta)\right| \geq \left(\int_0^1 \left|\sum_{n<N} r_n \,\mathrm{e}(n\vartheta)\right|^2 d\vartheta\right)^{1/2} = \sqrt{N}.$$

Shapiro in 1951 (see [42]) and then Rudin in 1959 (see [40]) gave examples of a sequence $(r_n)_{n\in\mathbb{N}}$ in $\{-1,+1\}^{\mathbb{N}}$ for which there exists a positive constant c such that for any positive integer N we have

$$\sup_{\vartheta\in[0,1]} \left|\sum_{n<N} r_n \,\mathrm{e}(n\vartheta)\right| \leq c\sqrt{N}$$

(see [42], [32], [2], or [36, Proposition 2.2.3] for $c = 2+\sqrt{2}$, [41] for $c = (2+\sqrt{2})\sqrt{\frac{3}{5}}$, and [11] for the proof that $c \geq \sqrt{6}$). This sequence, called Rudin–Shapiro sequence, can be defined for any $n \in \mathbb{N}$ by

$$r_n = (-1)^{\sum_{i\geq 1} \varepsilon_{i-1}(n)\varepsilon_i(n)}$$

(see [10, Theorem 4]), and it plays an important role in many problems in harmonic analysis (see for example [25, Chapitre X]) and in ergodic theory. In particular the existence of an ergodic transformation with Lebesgue spectrum of given finite multiplicity ℓ is an open problem for which the case $\ell = 1$ seems to be a very difficult question attributed to Banach. Queffélec showed in [38] (see also [37, Chapter VIII, section 2.2]) that the continuous part of the Rudin–Shapiro spectrum is Lebesgue with multiplicity equal to 2, and Lemańczyk, using more general sequences, obtained in [27] the Lebesgue spectrum with any given even multiplicity (see also [20]). Connes and Woods introduced in [15] the notion of approximate transitivity of a group action on a measure space in connection with some classification problems of factors of type III_0 in the theory of von Neumann algebras. El Abdalaoui and Lemańczyk proved in [19] that the Rudin–Shapiro dynamical system (as well as all the examples from [28] having even Lebesgue multiplicity) does not have the approximate transitivity property. The Rudin–Shapiro sequence is also linked to the one-dimensional Ising model [3], to Peano curves [32], and to brownian motion [26]. There are different ways to generalize Rudin–Shapiro sequences (see for example [1]), and in section 7 we will focus on the two following ways.

Definition 1. For any $\alpha \in \mathbb{R}$ and $\delta \in \mathbb{N}$, the sequence $(r_\delta(n,\alpha))_{n\in\mathbb{N}}$ defined for any $n \in \mathbb{N}$ by

$$r_\delta(n,\alpha) = \mathrm{e}\left(\alpha \sum_{k\geq\delta+1} \varepsilon_{k-\delta-1}(n)\,\varepsilon_k(n)\right)$$

is called a Rudin–Shapiro sequence of order δ.

Definition 2. For any $\alpha \in \mathbb{R}$ and $d \in \mathbb{N}$ with $d \geq 2$, the sequence $(R_d(n,\alpha))_{n\in\mathbb{N}}$ defined for any $n \in \mathbb{N}$ by

$$R_d(n,\alpha) = \mathrm{e}\left(\alpha \sum_{k\geq d-1} \varepsilon_{k-d+1}(n)\cdots\varepsilon_k(n)\right)$$

is called a Rudin–Shapiro sequence of degree d.

In [24] Kahane used generalized Rudin–Shapiro sequences of order δ with $\alpha = 1/2$ to construct a brownian quasi-screw in a finite-dimensional euclidian space.

2. Statement of the results

For $f : \mathbb{N} \to \mathbb{U}$ and any $\lambda \in \mathbb{N}$, let us denote by f_λ the q^λ-periodic function defined by

$$\forall n \in \{0,\ldots,q^\lambda - 1\},\ \forall k \in \mathbb{Z},\ f_\lambda(n + kq^\lambda) = f(n). \tag{1}$$

Definition 3. A function $f : \mathbb{N} \to \mathbb{U}$ has the *carry property* if, uniformly for $(\lambda,\kappa,\rho) \in \mathbb{N}^3$ with $\rho < \lambda$, the number of integers $0 \leq \ell < q^\lambda$ such that there exists $(k_1,k_2) \in \{0,\ldots,q^\kappa - 1\}^2$ with

$$f(\ell q^\kappa + k_1 + k_2)\,\overline{f(\ell q^\kappa + k_1)} \neq f_{\kappa+\rho}(\ell q^\kappa + k_1 + k_2)\,\overline{f_{\kappa+\rho}(\ell q^\kappa + k_1)} \tag{2}$$

is at most $O(q^{\lambda-\rho})$ where the implied constant may depend only on q and f.

In [31] we introduced a new method to study the distribution of prime numbers along a large class of sequences with digit properties and uniformly small discrete Fourier transforms in the following sense.

Definition 4. Given a nondecreasing function $\gamma : \mathbb{R} \to \mathbb{R}$ satisfying $\lim_{\lambda\to+\infty} \gamma(\lambda) = +\infty$ and $c > 0$, we denote by $\mathcal{F}_{\gamma,c}$ the set of functions $f : \mathbb{N} \to \mathbb{U}$ such that for $(\kappa,\lambda) \in \mathbb{N}^2$ with $\kappa \leq c\lambda$ and $t \in \mathbb{R}$,

$$\left| q^{-\lambda} \sum_{0\leq u<q^\lambda} f(uq^\kappa)\,\mathrm{e}\left(-ut\right)\right| \leq q^{-\gamma(\lambda)}. \tag{3}$$

The goal of this paper is to show that the method introduced in [31] can be adapted to the study of the distribution of squares for any base $q \geq 2$.

Theorem 1. *Let $\gamma : \mathbb{R} \to \mathbb{R}$ be a nondecreasing function satisfying $\lim_{\lambda\to+\infty} \gamma(\lambda) = +\infty$, and let $f : \mathbb{N} \to \mathbb{U}$ be a function satisfying Definition 3 and $f \in \mathcal{F}_{\gamma,c}$ for some $c \geq 18$ in Definition 4. Then for any $\vartheta \in \mathbb{R}$, we have*

$$\left| \sum_{0<n\leq x} f(n^2)\,\mathrm{e}(\vartheta n)\right| \ll_{f,q} (\log x)^{\omega(q)+2}\left(xq^{-\frac{\gamma(2\lfloor(3\log x)/(100\log q)\rfloor)}{56}}\right), \tag{4}$$

where the absolute constant implied depends only on f and q.

Remark. Theorem 1 gives a nontrivial result if

$$\liminf_{\lambda\to\infty} \frac{\gamma(\lambda)}{\log\lambda} > \frac{56\,(\omega(q)+2)}{\log q}. \tag{5}$$

3. Notations and preliminary tools

For $a \in \mathbb{Z}$ and $\kappa \in \mathbb{N}$, we denote by $\mathrm{r}_\kappa(a)$ the unique integer $r \in \{0,\dots,q^\kappa-1\}$ such that $a \equiv r \bmod q^\kappa$. More generally for integers $0 \le \kappa_1 \le \kappa_2$, we denote by $\mathrm{r}_{\kappa_1,\kappa_2}(a)$ the unique integer $u \in \{0,\dots,q^{\kappa_2-\kappa_1}-1\}$ such that $a = kq^{\kappa_2}+uq^{\kappa_1}+v$ for some $v \in \{0,\dots,q^{\kappa_1}-1\}$ and $k \in \mathbb{Z}$. We notice that we have $\mathrm{r}_{\kappa_1,\kappa_2}(a) = \left\lfloor \frac{\mathrm{r}_{\kappa_2}(a)}{q^{\kappa_1}} \right\rfloor$ and for any $u \in \{0,\dots,q^{\kappa_2-\kappa_1}-1\}$,

$$\mathrm{r}_{\kappa_1,\kappa_2}(a) = u \iff \frac{a}{q^{\kappa_2}} \in \left[\frac{u}{q^{\kappa_2-\kappa_1}}, \frac{u+1}{q^{\kappa_2-\kappa_1}}\right) + \mathbb{Z}. \tag{6}$$

For $a \ge 0$, $\mathrm{r}_\kappa(a)$ is the integer obtained from the κ least significant digits of a, while $\mathrm{r}_{\kappa_1,\kappa_2}(a)$ is the integer obtained using the digits of a of index in $\{\kappa_1,\dots,\kappa_2-1\}$.

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,

$$\chi_\alpha(x) = \lfloor x \rfloor - \lfloor x-\alpha \rfloor. \tag{7}$$

For any integer $H \ge 1$ it follows from [43, Theorem 19] that there exist real-valued trigonometric polynomials $A_{\alpha,H}(x)$ and $B_{\alpha,H}(x)$ such that for all $x \in \mathbb{R}$,

$$|\chi_\alpha(x) - A_{\alpha,H}(x)| \le B_{\alpha,H}(x), \tag{8}$$

where

$$A_{\alpha,H}(x) = \sum_{|h|\le H} a_h(\alpha,H)\,\mathrm{e}(hx), \qquad B_{\alpha,H}(x) = \sum_{|h|\le H} b_h(\alpha,H)\,\mathrm{e}(hx) \tag{9}$$

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

$$a_0(\alpha,H) = \alpha, \quad |a_h(\alpha,H)| \le \min\left(\alpha, \tfrac{1}{\pi|h|}\right), \quad |b_h(\alpha,H)| \le \tfrac{1}{H+1}. \tag{10}$$

For $(\alpha_1,\alpha_2) \in [0,1)^2$ we can detect the points in the rectangle $[0,\alpha_1)\times[0,\alpha_2)$ (modulo $\mathbb{Z}\times\mathbb{Z}$): for integers $H_1 \ge 1$, $H_2 \ge 1$, we have for all $(x,y) \in \mathbb{R}^2$,

$$\begin{aligned} &|\chi_{\alpha_1}(x)\chi_{\alpha_2}(y) - A_{\alpha_1,H_1}(x)A_{\alpha_2,H_2}(y)| \\ &\quad\le\ \chi_{\alpha_1}(x)B_{\alpha_2,H_2}(y) + B_{\alpha_1,H_1}(x)\chi_{\alpha_2}(y) + B_{\alpha_1,H_1}(x)B_{\alpha_2,H_2}(y), \end{aligned} \tag{11}$$

where $A_{\alpha,H}(.)$ and $B_{\alpha,H}(.)$ are the real-valued trigonometric polynomials defined by (9).

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

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

$$\left|\sum_{1\le n\le N} z_n\right|^2 \le \frac{N+kR-k}{R}\left(\sum_{1\le n\le N}|z_n|^2 + 2\sum_{1\le r<R}\left(1-\frac{r}{R}\right)\sum_{1\le n\le N-kr}\Re\left(z_{n+kr}\overline{z_n}\right)\right), \tag{12}$$

where $\Re(z)$ denotes the real part of z.

Proof. See, for example, [29, Lemma 17]. □

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 $\xi \in \mathbb{R}$:

$$\left| \sum_{L_1 < \ell \le L_2} \mathrm{e}(\ell \xi) \right| \le \min(L_2 - L_1, |\sin \pi \xi|^{-1}). \tag{13}$$

Lemmas 2 and 3 allow us to estimate on average the minimum arising from (13).

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

$$\sum_{0 \le n \le m-1} \min\left(U, \left|\sin \pi \tfrac{an+b}{m}\right|^{-1}\right) \le d \min\left(U, \left|\sin \pi \tfrac{d\,\|b/d\|}{m}\right|^{-1}\right) + \frac{2\,m}{\pi} \log(2\,m). \tag{14}$$

Proof. The result is trivial for $m = 1$. For $m \ge 2$ after using [30, Lemma 6] it suffices to observe that

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

Lemma 3. *Let $m \ge 1$ and $A \ge 1$ be integers, and let $b \in \mathbb{R}$. For any real number $U > 0$, we have*

$$\frac{1}{A} \sum_{1 \le a \le A} \sum_{0 \le n < m} \min\left(U, \left|\sin \pi \tfrac{an+b}{m}\right|^{-1}\right) \le \tau(m)\ U + \frac{2m}{\pi} \log(2m). \tag{15}$$

If $|b| \le \frac{1}{2}$, we have the sharper bound

$$\frac{1}{A} \sum_{1 \le a \le A} \sum_{0 \le n < m} \min\left(U, \left|\sin \pi \tfrac{an+b}{m}\right|^{-1}\right) \le \tau(m) \min\left(U, \left|\sin \pi \tfrac{b}{m}\right|^{-1}\right) + \frac{2m}{\pi} \log(2m). \tag{16}$$

Proof. Using (14), we have for all $b \in \mathbb{R}$,

$$\sum_{0 \le n < m} \min\left(U, \left|\sin \pi \tfrac{an+b}{m}\right|^{-1}\right) \le \gcd(a, m)\ U + \frac{2m}{\pi} \log(2m),$$

while for $|b| \le \frac{1}{2}$, we have $d\,\|b/d\| = |b|$ with $d = \gcd(a, m)$, and using (14), we get

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

It is enough to observe that

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

which implies (15) and (16) when $|b| \le \frac{1}{2}$. $\square$

In order to estimate quadratic Gauss sums, we use the following classical result.

Lemma 4. *For all $a, b, m \in \mathbb{Z}$ with $m \ge 1$, we have*

$$\left| \sum_{n=0}^{m-1} \mathrm{e}\left(\tfrac{an^2+bn}{m}\right) \right| \le \sqrt{2m \gcd(a, m)}. \tag{17}$$

Proof. This is [29, Proposition 2]. $\square$

For incomplete quadratic Gauss sums we have

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

$$\left| \sum_{n=n_0+1}^{n_0+N} \mathrm{e}\left(\tfrac{an^2+bn}{m}\right) \right| \leq \left(\tfrac{N}{m} + 1 + \tfrac{2}{\pi} \log \tfrac{2m}{\pi}\right) \sqrt{2m \gcd(a,m)}. \tag{18}$$

Proof. The following argument was already implicit in Vinogradov's works. For $m = 1$, the result is true. Assume that $m \geq 2$. There are $\lfloor N/m \rfloor$ complete sums which are majorized by $\sqrt{2m \gcd(a,m)}$. The remaining sum is either empty or of the form $S = \sum_{n=n_1+1}^{n_1+L} \mathrm{e}\left(\frac{an^2+bn}{m}\right)$ for some $n_1 \in \mathbb{Z}$ and $1 \leq L \leq m$. Detecting whether $n \equiv u \bmod m$ or not by $\frac{1}{m} \sum_{k=0}^{m-1} \mathrm{e}\left(k \frac{n-u}{m}\right)$, we get

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

thus

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

Applying Lemma 4 with b replaced by $b + k$ and observing (by convexity of $t \mapsto 1/\sin(\pi t/m)$) that

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

we obtain (18). □

Let $f : \mathbb{N} \to \mathbb{U}$ and $\lambda \in \mathbb{N}$, and let f_λ be defined by (1). The discrete Fourier transform of f_λ is defined for $t \in \mathbb{R}$ by

$$\widehat{f_\lambda}(t) = \frac{1}{q^\lambda} \sum_{0 \leq u < q^\lambda} f_\lambda(u) \, \mathrm{e}\left(-\frac{ut}{q^\lambda}\right) = \frac{1}{q^\lambda} \sum_{0 \leq u < q^\lambda} f(u) \, \mathrm{e}\left(-\frac{ut}{q^\lambda}\right). \tag{19}$$

For $\lambda \in \mathbb{N}$ and $t \in \mathbb{R}$, we have

$$\sum_{0 \leq h < q^\lambda} \left| \widehat{f_\lambda}(h+t) \right|^2 = 1 \tag{20}$$

so that, if f satisfies (3), then

$$1 = \sum_{0 \leq h < q^\lambda} \left| q^{-\lambda} \sum_{0 \leq u < q^\lambda} f(uq^\kappa) \, \mathrm{e}\left(\frac{-u(h+t)}{q^\lambda}\right) \right|^2 \leq \sum_{0 \leq h < q^\lambda} q^{-2\gamma(\lambda)} = q^{\lambda - 2\gamma(\lambda)}$$

and

$$\gamma(\lambda) \leq \frac{\lambda}{2}. \tag{21}$$

4. Carry propagation lemmas

Lemma 6. *Let* $(\nu,\nu')\in\mathbb{N}^2$ *with* $1\le\nu'\le 2\nu$. *For* $\mathcal{B}\subseteq\{0,\dots,q^{2\nu-\nu'}-1\}$, *the number* $\mathcal{N}$ *of integers* $n\in\{q^{\nu-1},\dots,q^{\nu}-1\}$ *such that* $n^2=a+q^{\nu'}b$ *with* $0\le a<q^{\nu'}$ *and* $b\in\mathcal{B}$ *satisfies*

$$\mathcal{N}\le \operatorname{card}\mathcal{B}+q^{\nu'/2}(\operatorname{card}\mathcal{B})^{1/2}.$$

Proof. We may assume $\operatorname{card}\mathcal{B}\ge 1$ (otherwise the result is true) and observe that for each $b\in\mathcal{B}$, we must count the n's such that $q^{\nu'}b\le n^2<q^{\nu'}(b+1)$. It follows that

$$\mathcal{N}\le\sum_{b\in\mathcal{B}}\left(1+q^{\nu'/2}\left(\sqrt{b+1}-\sqrt{b}\right)\right).$$

Since $t\mapsto\sqrt{t+1}-\sqrt{t}$ is decreasing, if $b_0<b_1<\cdots$ are the elements of $\mathcal{B}$, we have $b_j\ge j$, and

$$\mathcal{N}\le\operatorname{card}\mathcal{B}+q^{\nu'/2}\sum_{0\le j<\operatorname{card}\mathcal{B}}\left(\sqrt{j+1}-\sqrt{j}\right),$$

and the result follows. □

Lemma 7. *Let* $f:\mathbb{N}\to\mathbb{U}$ *satisfying Definition* 3, *and let* $(\nu,\kappa,\rho)\in\mathbb{N}^2$ *with* $3\rho<\nu<\kappa<\nu+2\rho$. *The set* $\mathcal{E}$ *of* $n\in\{q^{\nu-1},\dots,q^{\nu}-1\}$ *such that there exists* $k\in\{0,\dots,q^{\kappa}-1\}$ *with* $f(n^2+k)\,\overline{f(n^2)}\ne f_{\kappa+\rho}(n^2+k)\,\overline{f_{\kappa+\rho}(n^2)}$ *satisfies*

$$\operatorname{card}\mathcal{E}\ll_{f,q} q^{\nu-\frac{\rho}{2}}. \tag{22}$$

Proof. We apply Definition 3 with $\lambda=2\nu-\kappa$. Since $3\rho<\nu$ and $\kappa<\nu+2\rho$, the condition $\rho<\lambda$ is satisfied. Let $\mathcal{B}$ be the set of $\ell<q^{\lambda}$ such that there exists $(k_1,k_2)\in\{0,\dots,q^{\kappa}-1\}^2$ for which (2) is true. By Definition 3 we have $\operatorname{card}\mathcal{B}\ll_{f,q}q^{\lambda-\rho}$. We need to count $n\in\{q^{\nu-1},\dots,q^{\nu}-1\}$ such that n^2 is of the form $n^2=k_1+q^{\kappa}\ell$ with $\ell\in\mathcal{B}$. Applying Lemma 6 with $\nu'=\kappa$, we get

$$\operatorname{card}\mathcal{E}\ll\operatorname{card}\mathcal{B}+q^{\nu'/2}(\operatorname{card}\mathcal{B})^{1/2}\ll_{f,q}q^{\lambda-\rho}+q^{\frac{\kappa+\lambda-\rho}{2}}\ll q^{\nu-\frac{\rho}{2}},$$

which gives (22). □

For integers $0\le\nu_1\le\nu_2$ and f_{ν_1} and f_{ν_2} defined by (19), we write

$$f_{\nu_1,\nu_2}=f_{\nu_2}\overline{f_{\nu_1}}. \tag{23}$$

Lemma 8. *Let* $f:\mathbb{N}\to\mathbb{U}$ *satisfying Definition* 3 *and* $\nu\ge 0$. *For* $\nu_0\le\nu_1\le\nu\le\nu_2$, *the set* $\mathcal{E}$ *of integers* $n\in\{q^{\nu-1},\dots,q^{\nu}-1\}$ *such that*

$$f_{\nu_1,\nu_2}(n^2)\ne f_{\nu_1,\nu_2}(q^{\nu_0}\,\mathrm{r}_{\nu_0,\nu_2}(n^2))$$

satisfies

$$\operatorname{card}\mathcal{E}\ll_{f,q}q^{\nu-\nu_1+\nu_0}+q^{\frac{\nu_2}{2}+\nu_2-\nu_1}\log q^{\nu_2}. \tag{24}$$

Proof. Let $\mathcal{B}$ be the set of $\ell\in\{0,\dots,q^{\nu_2-\nu_0}-1\}$ for which there exists $(k_1,k_2)\in\{0,\dots,q^{\nu_0}-1\}^2$ with

$$f_{\nu_1,\nu_2}(q^{\nu_0}\ell+k_1+k_2)\ne f_{\nu_1,\nu_2}(q^{\nu_0}\ell+k_1),$$

i.e.,

$$f_{\nu_2}(q^{\nu_0}\ell+k_1+k_2)\;\overline{f_{\nu_2}(q^{\nu_0}\ell+k_1)}\ne f_{\nu_1}(q^{\nu_0}\ell+k_1+k_2)\;\overline{f_{\nu_1}(q^{\nu_0}\ell+k_1)}.$$

For $0\le\ell\le q^{\nu_2-\nu_0}-2$, we have $0\le q^{\nu_0}\ell+k_1+k_2\le q^{\nu_2}-2$. Therefore we have $f_{\nu_2}(q^{\nu_0}\ell+k_1+k_2)=f(q^{\nu_0}\ell+k_1+k_2)$ and $f_{\nu_2}(q^{\nu_0}\ell+k_1)=f(q^{\nu_0}\ell+k_1)$ for

$0 \le \ell < q^{\nu_2-\nu_0}$ except possibly if $\ell = q^{\nu_2-\nu_0} - 1$. Since f satisfies Definition 3, it follows that $\operatorname{card}\mathcal{B} \ll_{f,q} q^{\nu_2-\nu_0-(\nu_1-\nu_0)} = q^{\nu_2-\nu_1}$. Observing that $n^2 = \mathrm{r}_{0,\nu_0}(n^2) + q^{\nu_0}\,\mathrm{r}_{\nu_0,\nu_2}(n^2) + q^{\nu_2}\,\mathrm{r}_{\nu_2,2\nu}(n^2)$, we notice that $\mathcal{E} \subseteq \mathcal{E}'$ where $\mathcal{E}'$ is the set of n's such that $\mathrm{r}_{\nu_0,\nu_2}(n^2) \in \mathcal{B}$. Then we can write

$$\operatorname{card}\mathcal{E}' = \sum_{\ell\in\mathcal{B}} \operatorname{card}\{n \in \{q^{\nu-1},\dots,q^{\nu}-1\},\ \mathrm{r}_{\nu_0,\nu_2}(n^2) = \ell\},$$

which by (6) and (7) can be written

$$\operatorname{card}\mathcal{E}' = \sum_{\ell\in\mathcal{B}}\sum_{n} \chi_{q^{\nu_0-\nu_2}}\left(\frac{n^2}{q^{\nu_2}} - \frac{\ell}{q^{\nu_2-\nu_0}}\right).$$

Using (8) with $H = q^{\nu_2-\nu_0}$, it follows that there exists a_h and b_h satisfying (10) such that

$$\operatorname{card}\mathcal{E}' \le \sum_{\ell\in\mathcal{B}}\sum_{n}\sum_{|h|\le H} \big(a_h(q^{\nu_0-\nu_2},H) + b_h(q^{\nu_0-\nu_2},H)\big)\,\mathrm{e}\left(\frac{hn^2}{q^{\nu_2}} - \frac{h\ell}{q^{\nu_2-\nu_0}}\right).$$

The contribution of the terms $h = 0$ is bounded by

$$q^{\nu+\nu_0-\nu_2}\operatorname{card}\mathcal{B} \ll_{f,q} q^{\nu+\nu_0-\nu_1}.$$

Exchanging the order of summations and using the bounds given by (10), namely $|a_h| \le q^{\nu_0-\nu_2}$ and $|b_h| \le H^{-1} = q^{\nu_0-\nu_2}$, we obtain the upper bound

$$\operatorname{card}\mathcal{E}' \ll_{f,q} q^{\nu+\nu_0-\nu_1} + \frac{\operatorname{card}\mathcal{B}}{q^{\nu_2-\nu_0}} \sum_{1\le|h|\le q^{\nu_2-\nu_0}} \left|\sum_{n}\mathrm{e}\left(\frac{hn^2}{q^{\nu_2}}\right)\right|.$$

By (18) this gives

$$\operatorname{card}\mathcal{E}' \ll_{f,q} q^{\nu+\nu_0-\nu_1} + \frac{q^{\nu_2-\nu_1}}{q^{\nu_2-\nu_0}} \sum_{1\le h\le q^{\nu_2-\nu_0}} (\log q^{\nu_2})\sqrt{\gcd(h,q^{\nu_2})q^{\nu_2}}.$$

For any $A \ge 1$ and $\lambda \in \mathbb{N}$, we have

$$\sum_{1\le a\le A}\sqrt{\gcd(a,q^{\lambda})} \le \sum_{\substack{d\,|\,q^{\lambda}\\ d\le A}} d^{1/2} \sum_{\substack{1\le a\le A\\ a\equiv 0 \bmod d}} 1 \le \sum_{\substack{d\,|\,q^{\lambda}\\ d\le A}} d^{1/2}\,\frac{A}{d} \le \sum_{d\,|\,q^{\lambda}} \frac{A}{d^{1/2}}$$

so that, observing that $n \mapsto \sum_{d\,|\,n} d^{-1/2}$ is multiplicative, we get

$$A^{-1}\sum_{1\le a\le A}\sqrt{\gcd(a,q^{\lambda})} \le \sum_{d\,|\,q^{\lambda}}\frac{1}{d^{1/2}} \le C_q = \prod_{p\,|\,q}\sum_{k=0}^{\infty}\frac{1}{p^{k/2}} = \prod_{p\,|\,q}(1-p^{-1/2})^{-1}, \tag{25}$$

and it follows that

$$\operatorname{card}\mathcal{E}' \ll_{f,q} q^{\nu+\nu_0-\nu_1} + q^{\frac{\nu_2}{2}+\nu_2-\nu_1}\log q^{\nu_2},$$

which gives (24). □

5. Exponential sums

We take $\gamma : \mathbb{R} \to \mathbb{R}$ a nondecreasing function satisfying $\lim_{\lambda\to+\infty} \gamma(\lambda) = +\infty$, $c \geq c_0$ (to be chosen later in (57)) and $f : \mathbb{N} \to \mathbb{U}$ a function satisfying Definition 3 and belonging to the set $\mathcal{F}_{\gamma,c}$ in Definition 4.

Let $N \geq 1$, and let ν be the unique integer such that $q^{\nu-1} \leq N < q^{\nu}$. Let $\vartheta \in \mathbb{R}$ and

$$S_0 = \sum_{N/2<n\leq N} f(n^2)\,\mathrm{e}(\vartheta n).$$

Our aim is to prove uniformly for all $\vartheta \in \mathbb{R}$ that

$$|S_0| \ll_{f,q} \nu^{(\omega(q)+2)/4} q^{\nu-\frac{\gamma(2\lfloor 7\nu/179\rfloor)}{56}}. \tag{26}$$

Let $\rho \in \mathbb{N}$ such that

$$3 \leq \rho \leq \tfrac{\nu}{18}, \tag{27}$$

and choose

$$R = q^{\rho}. \tag{28}$$

Applying Lemma 1 with $k = 1$, we get

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

with

$$S_1(r) = \sum_{n\in I_1(N,r)} f((n+r)^2)\overline{f(n^2)}\,\mathrm{e}(\vartheta r),$$

where $I_1(N,r) = (N/2, N] \cap (N/2 - r, N - r]$. Let

$$\nu_2 = \nu + 2\rho. \tag{29}$$

If f satisfies the carry property explained in Definition 3, then by Lemma 7, applied with (κ, ρ) replaced by $(\nu + \rho + 2, \rho - 2)$, the number of $n \in (N/2, N]$ for which $f(n^2 + 2rn + r^2)\overline{f(n^2)} \neq f_{\nu_2}(n^2 + 2rn + r^2)\overline{f_{\nu_2}(n^2)}$ is $O_{f,q}(q^{\nu-\frac{\rho}{2}})$. Hence

$$S_1(r) = S_1'(r) + O_{f,q}(q^{\nu-\frac{\rho}{2}}), \tag{30}$$

where

$$S_1'(r) = \sum_{n\in I_1(N,r)} f_{\nu_2}((n+r)^2)\overline{f_{\nu_2}(n^2)}\,\mathrm{e}(\vartheta r).$$

Using (30) and the Cauchy–Schwarz inequality for the summation over r, this leads to

$$|S_0|^4 \ll_{f,q} q^{4\nu-\rho} + \frac{N^4}{R^2} + \frac{N^2}{R^2} R \sum_{1\leq r<R} |S_1'(r)|^2.$$

Let

$$\nu_1 = \nu - 2\rho \tag{31}$$

and

$$S = R^2 = q^{2\rho}. \tag{32}$$

We have $1 \leq q^{\nu_1} S \ll N$. Applying Lemma 1 with $k = q^{\nu_1}$ and S in place of R and then summing over r, we obtain

$$|S_0|^4 \ll_{f,q} q^{4\nu-\rho} + \frac{N^4}{R^2} + \frac{N^4}{S} + \frac{N^3}{RS}\Re(S_2)$$

with

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

and

$$S_2'(r,s) = \sum_{n\in I_2(N,r,s)} f_{\nu_2}((n+r+sq^{\nu_1})^2)\overline{f_{\nu_2}((n+r)^2)f_{\nu_2}((n+sq^{\nu_1})^2)}f_{\nu_2}(n^2),$$

where $I_2(N,r,s) = I_1(N,r)\cap(I_1(N,r)-sq_1^{\nu})$ is an interval included in $(N/2,N]$. Observing that $f_{\nu_1}((n+r+sq^{\nu_1})^2) = f_{\nu_1}((n+r)^2)$ and $f_{\nu_1}((n+sq^{\nu_1})^2) = f_{\nu_1}(n^2)$ so that

$$\overline{f_{\nu_1}((n+r+sq^{\nu_1})^2)}f_{\nu_1}((n+r)^2) = f_{\nu_1}((n+r+sq^{\nu_1})^2)\overline{f_{\nu_1}((n+r)^2)} = 1$$

and using (23), we can write

$$S_2'(r,s) = \sum_{n\in I_2(N,r,s)} f_{\nu_1,\nu_2}((n+r+sq^{\nu_1})^2)\overline{f_{\nu_1,\nu_2}((n+r)^2)f_{\nu_1,\nu_2}((n+sq^{\nu_1})^2)}f_{\nu_1,\nu_2}(n^2).$$

For $\nu_0\le\nu_1$, let us denote by $\mathcal{E}_{\nu_0,\nu_1,\nu_2}$ the set of $n\in(N/2,N]$ such that

$$f_{\nu_1,\nu_2}(n^2)\ne f_{\nu_1,\nu_2}(q^{\nu_0}\,\mathrm{r}_{\nu_0,\nu_2}(n^2)).$$

For $0\le r<R$ and $0\le s<S$, the set $\mathcal{E}_{\nu_0,\nu_1,\nu_2}(r,s)$ of $n\in I_2(N,r,s)$ such that

$$f_{\nu_1,\nu_2}((n+r+sq^{\nu_1})^2)\ne f_{\nu_1,\nu_2}(q^{\nu_0}\,\mathrm{r}_{\nu_0,\nu_2}((n+r+sq^{\nu_1})^2)).$$

Observing that $n+r+sq^{\nu_1}\in(N/2,N]$, using Lemma 8, (27), (29), and (31), we obtain

$$\operatorname{card}\mathcal{E}_{\nu_0,\nu_1,\nu_2}(r,s)\le\operatorname{card}\mathcal{E}_{\nu_0,\nu_1,\nu_2}\ll_{f,q} q^{\nu-\nu_1+\nu_0}+q^{\frac{\nu}{2}+5\rho}\nu\log q.$$

The set $\mathcal{E}_{\nu_0,\nu_1,\nu_2}$ is a set of exceptions: if ν_0 is taken sufficiently small, the function f_{ν_1,ν_2} will depend on the digits of index in $\nu_0,\dots,\nu_2-1$, except for $n\in\mathcal{E}_{\nu_0,\nu_1,\nu_2}$. Of course if $\nu_0=0$, we have $\mathcal{E}_{\nu_0,\nu_1,\nu_2}=\emptyset$, but we want to choose ν_0 more carefully so that this set is still small enough. More precisely, let $\rho'\in\mathbb{N}$ to be chosen later such that

$$0\le\rho'\le\rho. \tag{33}$$

Since f is a function satisfying Definition 3, we have by taking

$$\nu_0=\nu_1-2\rho' \tag{34}$$

and using (27) and (31),

$$\operatorname{card}\mathcal{E}_{\nu_0,\nu_1,\nu_2}(r,s)\ll_{f,q}\ q^{\nu-2\rho'}. \tag{35}$$

Remark. A direct argument depending on a better knowledge of f might permit us to choose a greater value of ν_0, leading to a sharper final estimate for such a more specific function f.

This leads to

$$|S_0|^4\ll_{f,q} q^{4\nu-\rho}+q^{4\nu-2\rho'}+\frac{N^4}{R^2}+\frac{N^3}{RS}\Re(S_3) \tag{36}$$

with

$$S_3 = \sum_{1\le r<R}\sum_{1\le s<S}\left(1-\frac{s}{S}\right)\ S_3'(r,s) \tag{37}$$

and

$$S_3'(r,s) = \sum_{n\in I_2(N,r,s)} g(\mathrm{r}_{\nu_0,\nu_2}\left((n+r+sq^{\nu_1})^2\right))\overline{g(\mathrm{r}_{\nu_0,\nu_2}\left((n+r)^2\right))}$$
$$\overline{g(\mathrm{r}_{\nu_0,\nu_2}\left((n+sq^{\nu_1})^2\right))}g(\mathrm{r}_{\nu_0,\nu_2}\left(n^2\right))$$

with

$$g(k) = f_{\nu_1,\nu_2}(q^{\nu_0}k). \tag{38}$$

If $\mathrm{r}_{\nu_0,\nu_2}(n^2) = u_0$, since by (27), (29), and (31), we have $2\nu_1 \geq \nu_2$, it follows that

$$\mathrm{r}_{\nu_0,\nu_2}\left((n+sq^{\nu_1})^2\right) = \mathrm{r}_{\nu_0,\nu_2}\left(q^{\nu_0}u_0 + 2snq^{\nu_1}\right) = \mathrm{r}_{\nu_2-\nu_0}\left(u_0 + 2snq^{\nu_1-\nu_0}\right).$$

Similarly, if $\mathrm{r}_{\nu_0,\nu_2}((n+r)^2) = u_1$, we get

$$\begin{aligned}\mathrm{r}_{\nu_0,\nu_2}\left((n+r+sq^{\nu_1})^2\right) &= \mathrm{r}_{\nu_0,\nu_2}\left(q^{\nu_0}u_1 + 2snq^{\nu_1} + 2srq^{\nu_1}\right)\\ &= \mathrm{r}_{\nu_2-\nu_0}\left(u_1 + 2snq^{\nu_1-\nu_0} + 2srq^{\nu_1-\nu_0}\right).\end{aligned}$$

By (38), g is periodic of period $q^{\nu_2-\nu_0}$. Using (6), we can write

$$\begin{aligned}S_3'(r,s) \quad = \quad & \sum_{n\in I_2(N,r,s)} \sum_{\substack{0\leq u_0<q^{\nu_2-\nu_0}\\ 0\leq u_1<q^{\nu_2-\nu_0}}} \\ & g(u_1 + 2q^{\nu_1-\nu_0}sn + 2q^{\nu_1-\nu_0}rs)\overline{g(u_0+2q^{\nu_1-\nu_0}sn)g(u_1)}g(u_0)\\ & \chi_{q^{\nu_0-\nu_2}}\left(\frac{n^2}{q^{\nu_2}} - \frac{u_0}{q^{\nu_2-\nu_0}}\right)\chi_{q^{\nu_0-\nu_2}}\left(\frac{(n+r)^2}{q^{\nu_2}} - \frac{u_1}{q^{\nu_2-\nu_0}}\right),\end{aligned}$$

where $\chi_{q^{\nu_0-\nu_2}}$ is defined by (7) with $\alpha = q^{\nu_0-\nu_2}$. Let H be an integer satisfying

$$q^{\nu_2-\nu_0} \leq H \leq q^{\nu} \tag{39}$$

to be chosen later. Using (11), we have

$$S_3'(r,s) = S_4(r,s) + O(E_4(r,0)) + O(E_4(0,r)) + O(E_4'(r)) \tag{40}$$

with the main term $S_4(r,s)$ equal to

$$\sum_{n\in I_2(N,r,s)} \sum_{\substack{0\leq u_0<q^{\nu_2-\nu_0}\\ 0\leq u_1<q^{\nu_2-\nu_0}}} g(u_1 + 2q^{\nu_1-\nu_0}sn + 2q^{\nu_1-\nu_0}rs)\overline{g(u_0+2q^{\nu_1-\nu_0}sn)g(u_1)}g(u_0)$$
$$A_{q^{\nu_0-\nu_2},H}\left(\frac{n^2}{q^{\nu_2}} - \frac{u_0}{q^{\nu_2-\nu_0}}\right)A_{q^{\nu_0-\nu_2},H}\left(\frac{(n+r)^2}{q^{\nu_2}} - \frac{u_1}{q^{\nu_2-\nu_0}}\right).$$

For the error terms, since $\chi = \chi_{q^{\nu_0-\nu_2}} \geq 0$ and $B = B_{q^{\nu_0-\nu_2},H} \geq 0$, it is possible to extend the summation over n to the full interval, removing the dependence in s:

$$E_4(r,r') = \sum_{N/2<n\leq N} \sum_{\substack{0\leq u_0<q^{\nu_2-\nu_0}\\ 0\leq u_1<q^{\nu_2-\nu_0}}} B\left(\frac{(n+r)^2}{q^{\nu_2}} - \frac{u_0}{q^{\nu_2-\nu_0}}\right)\chi\left(\frac{(n+r')^2}{q^{\nu_2}} - \frac{u_1}{q^{\nu_2-\nu_0}}\right),$$

$$E_4'(r) = \sum_{N/2<n\leq N} \sum_{\substack{0\leq u_0<q^{\nu_2-\nu_0}\\ 0\leq u_1<q^{\nu_2-\nu_0}}} B\left(\frac{n^2}{q^{\nu_2}} - \frac{u_0}{q^{\nu_2-\nu_0}}\right)B\left(\frac{(n+r)^2}{q^{\nu_2}} - \frac{u_1}{q^{\nu_2-\nu_0}}\right).$$

5.1. **Estimate of $E_4(r,r')$.**

Since for any $t\in\mathbb{R}$ we have $\sum_{0\le u_1<q^{\nu_2-\nu_0}}\chi_{q^{\nu_0-\nu_2}}\left(t-\frac{u_1}{q^{\nu_2-\nu_0}}\right)=1$, this gives

$$E_4(r,r')=\sum_{N/2<n\le N}\ \sum_{0\le u_0<q^{\nu_2-\nu_0}} B_{q^{\nu_0-\nu_2},H}\left(\frac{(n+r)^2}{q^{\nu_2}}-\frac{u_0}{q^{\nu_2-\nu_0}}\right),$$

which by (9) gives

$$E_4(r,r')=\sum_{|h_0|\le H} b_{h_0}(q^{\nu_0-\nu_2},H)\sum_{N/2<n\le N}\ \sum_{0\le u_0<q^{\nu_2-\nu_0}} \mathrm{e}\left(\frac{h_0(n+r)^2}{q^{\nu_2}}-\frac{h_0u_0}{q^{\nu_2-\nu_0}}\right).$$

By (10) we have $|b_{h_0}(q^{\nu_0-\nu_2},H)|\le H^{-1}$, and we observe that

$$\frac{1}{q^{\nu_2-\nu_0}}\sum_{0\le u_0<q^{\nu_2-\nu_0}}\mathrm{e}\left(-\frac{h_0u_0}{q^{\nu_2-\nu_0}}\right)=\begin{cases}1 & \text{if } h_0\equiv 0 \bmod q^{\nu_2-\nu_0},\\ 0 & \text{if } h_0\not\equiv 0 \bmod q^{\nu_2-\nu_0},\end{cases}$$

so that, writing $h_0=h_0'q^{\nu_2-\nu_0}$, we get

$$|E_4(r,r')|\ll E_5(r) \tag{41}$$

with

$$E_5(r)=\frac{q^{\nu_2-\nu_0}}{H}\sum_{|h_0'|\le H/q^{\nu_2-\nu_0}}\left|\sum_{N/2<n\le N}\mathrm{e}\left(\frac{h_0'(n+r)^2}{q^{\nu_0}}\right)\right|.$$

It remains to estimate $E_5(r)$. By (27) and (39) for $|h_0'|\le H/q^{\nu_2-\nu_0}$, we have $h_0'\equiv 0 \bmod q^{\nu_0}$ if and only if $h_0'=0$. Using (18), we have uniformly for $r\in\mathbb{Z}$,

$$E_5(r)\ll\frac{q^{\nu+\nu_2-\nu_0}}{H}+\frac{q^{\nu_2-\nu_0}}{H}\sum_{0<|h'|\le H/q^{\nu_2-\nu_0}}\left(q^{\nu-\nu_0}+\log q^{\nu_0}\right)\sqrt{\gcd(h',q^{\nu_0})q^{\nu_0}},$$

and by (25)

$$\sum_{0<|h'|\le H/q^{\nu_2-\nu_0}}\sqrt{\gcd(h',q^{\nu_0})}\ll_q H/q^{\nu_2-\nu_0},$$

which, for all integers H with $q^{\nu_2-\nu_0}\le H\le q^{\nu}$, leads to

$$E_5(r)\ll_q\frac{q^{\nu+\nu_2-\nu_0}}{H}+q^{\nu_0/2}\left(q^{\nu-\nu_0}+\log q^{\nu_0}\right).$$

Choosing

$$H=q^{\nu_2-\nu_0+2\rho}, \tag{42}$$

by (34), (31), (29), and (27) we get

$$|E_5(r)|\ll_q q^{\nu-2\rho}. \tag{43}$$

5.2. **Estimate of $E_4'(r)$.** We have

$$E_4'(r)=\sum_{|h_0|\le H}\sum_{|h_1|\le H} b_{h_0}(q^{\nu_0-\nu_2},H)\, b_{h_1}(q^{\nu_0-\nu_2},H)$$
$$\sum_{N/2<n\le N}\ \sum_{\substack{0\le u_0<q^{\nu_2-\nu_0}\\0\le u_1<q^{\nu_2-\nu_0}}}\mathrm{e}\left(h_0\frac{n^2}{q^{\nu_2}}-h_0\frac{u_0}{q^{\nu_2-\nu_0}}\right)\mathrm{e}\left(h_1\frac{(n+r)^2}{q^{\nu_2}}-h_1\frac{u_1}{q^{\nu_2-\nu_0}}\right).$$

We observe that for $h_0 \not\equiv 0 \bmod q^{\nu_2-\nu_0}$ we have $\sum_{0\le u_0<q^{\nu_2-\nu_0}} \mathrm{e}\left(-h_0 \frac{u_0}{q^{\nu_2-\nu_0}}\right) = 0$ and similarly for h_1. Hence we may assume $h_0 \equiv h_1 \equiv 0 \bmod q^{\nu_2-\nu_0}$. Writing $h_0 = h_0' q^{\nu_2-\nu_0}$ and $h_1 = h_1' q^{\nu_2-\nu_0}$ and using $|b_h(H)| \le \frac{1}{H}$ (by (10)), we get

$$|E_4'(r)| \ll \frac{q^{2(\nu_2-\nu_0)}}{H^2} \sum_{\substack{|h_0'|\le H/q^{\nu_2-\nu_0}\\ |h_1'|\le H/q^{\nu_2-\nu_0}}} \left| \sum_{N/2<n\le N} \mathrm{e}\left(\frac{(h_0'+h_1')n^2 + 2h_1' rn}{q^{\nu_0}}\right)\right|.$$

The contribution to $E_4'(r)$ of the terms for which $h_0'+h_1' = 0$ is majorized by

$$H^{-2}\ q^{2(\nu_2-\nu_0)} \sum_{|h_1'|\le H/q^{\nu_2-\nu_0}} \min\left(N, \left|\sin \pi \tfrac{2h_1' r}{q^{\nu_0}}\right|^{-1}\right).$$

Since $1 \le r < q^\rho$, by (42), (34), (31), (27), so that (33), we have

$$r(1+2Hq^{\nu_0-\nu_2}) \le q^\rho(1+2q^{2\rho}) < q^{\nu_0},$$

and the values of $2h_1' r$ are all distinct modulo q^{ν_0} in the summation over h_1' above. Therefore

$$\sum_{|h_1'|\le H/q^{\nu_2-\nu_0}} \min\left(N, \left|\sin \pi \tfrac{2h_1' r}{q^{\nu_0}}\right|^{-1}\right) \le \sum_{\ell \bmod q^{\nu_0}} \min\left(N, \left|\sin \pi \tfrac{\ell}{q^{\nu_0}}\right|^{-1}\right),$$

and we conclude by (14) that the contribution to $E_4'(r)$ of the terms for which $h_0'+h_1' = 0$ is majorized by

$$H^{-2}\ q^{2(\nu_2-\nu_0)}(N + q^{\nu_0}\log q^{\nu_0}) \ll_q \nu_0\ H^{-2} q^{\nu+2(\nu_2-\nu_0)}.$$

Using (18), the contribution to $E_4'(r)$ of the terms for which $h_0'+h_1' \ne 0$ is

$$\ll H^{-2}\ q^{2(\nu_2-\nu_0)} \sum_{h_0'+h_1'\ne 0} \left(q^{\nu-\nu_0} + \log q^{\nu_0}\right) \sqrt{\gcd(h_0'+h_1', q^{\nu_0})q^{\nu_0}},$$

which is, writing $h' = h_0' + h_1'$,

$$\ll q^{\nu_0/2}\left(q^{\nu-\nu_0} + \log q^{\nu_0}\right) H^{-1} q^{\nu_2-\nu_0} \sum_{0<|h'|\le 2H/q^{\nu_2-\nu_0}} \sqrt{\gcd(h', q^{\nu_0})}.$$

By (25), for all integers H with $q^{\nu_2-\nu_0} \le H \le q^{\nu_0}$, this is

$$\ll_q q^{\nu_0/2}\left(q^{\nu-\nu_0} + \log q^{\nu_0}\right),$$

so that we obtain the estimate

$$|E_4'(r)| \ll_q \nu_0\ H^{-2} q^{\nu+2(\nu_2-\nu_0)} + q^{\nu-\frac{\nu_0}{2}} + \nu_0\, q^{\nu_0/2}.$$

Using (42), (34), (31), (29), and (27), we get

$$|E_4'(r)| \ll_q \nu\ q^{\nu-2\rho}. \tag{44}$$

By (40), (41), (43), and (44), we obtain

$$S_3'(r,s) = S_4(r,s) + O_q(\nu\, q^{\nu-2\rho}). \tag{45}$$

5.3. **Estimate of $S_4(r,s)$.** We have

$$S_4(r,s) = \sum_{|h_0|\le H}\sum_{|h_1|\le H} a_{h_0}(q^{\nu_0-\nu_2},H)\ a_{h_1}(q^{\nu_0-\nu_2},H) \sum_{n\in I_2(N,r,s)} \sum_{\substack{0\le u_0<q^{\nu_2-\nu_0}\\ 0\le u_1<q^{\nu_2-\nu_0}}} g(u_1+2q^{\nu_1-\nu_0}sn+2q^{\nu_1-\nu_0}rs)\overline{g(u_0+2q^{\nu_1-\nu_0}sn)g(u_1)}g(u_0)\ \mathrm{e}\left(h_0\frac{n^2}{q^{\nu_2}}-h_0\frac{u_0}{q^{\nu_2-\nu_0}}\right)\mathrm{e}\left(h_1\frac{(n+r)^2}{q^{\nu_2}}-h_1\frac{u_1}{q^{\nu_2-\nu_0}}\right).$$

We write $u_0+2snq^{\nu_1-\nu_0}\equiv u_2 \bmod q^{\nu_2-\nu_0}$ and $u_1+2snq^{\nu_1-\nu_0}+2rsq^{\nu_1-\nu_0}\equiv u_3 \bmod q^{\nu_2-\nu_0}$. This gives

$$S_4(r,s) = \sum_{|h_0|\le H}\sum_{|h_1|\le H} a_{h_0}(q^{\nu_0-\nu_2},H)\ a_{h_1}(q^{\nu_0-\nu_2},H)\frac{1}{q^{2(\nu_2-\nu_0)}} \sum_{\substack{0\le h_2<q^{\nu_2-\nu_0}\\ 0\le h_3<q^{\nu_2-\nu_0}}} \sum_{\substack{0\le u_0<q^{\nu_2-\nu_0}\\ 0\le u_1<q^{\nu_2-\nu_0}}} \mathrm{e}\left(\frac{-h_0u_0}{q^{\nu_2-\nu_0}}\right)\mathrm{e}\left(\frac{-h_1u_1}{q^{\nu_2-\nu_0}}\right)\overline{g(u_1)}g(u_0) \sum_{\substack{0\le u_2<q^{\nu_2-\nu_0}\\ 0\le u_3<q^{\nu_2-\nu_0}}} g(u_3)\overline{g(u_2)} \sum_{n\in I_2(N,r,s)} \mathrm{e}\left(\frac{h_0n^2+h_1(n+r)^2}{q^{\nu_2}}\right)\mathrm{e}\left(h_2\frac{u_0+2snq^{\nu_1-\nu_0}-u_2}{q^{\nu_2-\nu_0}}\right) \mathrm{e}\left(h_3\frac{u_1+2snq^{\nu_1-\nu_0}+2rsq^{\nu_1-\nu_0}-u_3}{q^{\nu_2-\nu_0}}\right),$$

and we obtain

$$S_4(r,s) = q^{2(\nu_2-\nu_0)}\sum_{|h_0|\le H}\sum_{|h_1|\le H} a_{h_0}(q^{\nu_0-\nu_2},H)a_{h_1}(q^{\nu_0-\nu_2},H) \sum_{0\le h_2<q^{\nu_2-\nu_0}}\sum_{0\le h_3<q^{\nu_2-\nu_0}} \mathrm{e}\left(\frac{2h_3rs}{q^{\nu_2-\nu_1}}\right)\widehat{g}(h_0-h_2)\ \overline{\widehat{g}(h_3-h_1)}\ \overline{\widehat{g}(-h_2)}\ \widehat{g}(h_3) \sum_{n\in I_2(N,r,s)} \mathrm{e}\left(\frac{h_0n^2+h_1(n+r)^2+2sq^{\nu_1}(h_2+h_3)n}{q^{\nu_2}}\right),$$

where

$$\widehat{g}(h) = \frac{1}{q^{\nu_2-\nu_0}}\sum_{0\le u<q^{\nu_2-\nu_0}} g(u)\,\mathrm{e}\left(-\frac{uh}{q^{\nu_2-\nu_0}}\right) \tag{46}$$

is the discrete Fourier transform related to g defined by (19).

We write

$$S_4(r,s) = S_4'(r,s)+S_4''(r,s), \tag{47}$$

where $S_4'(r,s)$ denotes the contribution to $S_4(r,s)$ of the terms for which $h_0+h_1=0$, and $S_4''(r,s)$ denotes the contribution to $S_4(r,s)$ of the terms for which $h_0+h_1\neq 0$.

5.3.1. *Contribution of $S_4'(r,s)$.* We have

$$S_4'(r,s) \le q^{2(\nu_2-\nu_0)} \sum_{|h_1|\le H} \left|a_{h_1}(q^{\nu_0-\nu_2},H)\right|^2 \sum_{0\le h_2<q^{\nu_2-\nu_0}} \sum_{0\le h_3<q^{\nu_2-\nu_0}} |\widehat{g}(-h_1-h_2)\ \widehat{g}(h_3-h_1)\ \widehat{g}(-h_2)\ \widehat{g}(h_3)| \left|\sum_{n\in I_2(N,r,s)} \mathrm{e}\left(\frac{2h_1r+2(h_2+h_3)sq^{\nu_1}}{q^{\nu_2}}n\right)\right|.$$

When h_2 runs over a complete set of residues modulo $q^{\nu_2-\nu_0}$, so does $h = h_2+h_3$. Thus, by periodicity modulo $q^{\nu_2-\nu_0}$, we have

$$|S_4'(r,s)| \le S_5(r,s) \tag{48}$$

with

$$S_5(r,s) = q^{2(\nu_2-\nu_0)} \sum_{|h_1|\le H} \left|a_{h_1}(q^{\nu_0-\nu_2},H)\right|^2 \sum_{0\le h<q^{\nu_2-\nu_0}} \min\left(q^{\nu}, \left|\sin\pi\frac{2h_1r+2hsq^{\nu_1}}{q^{\nu_2}}\right|^{-1}\right) S_6(h,h_1)$$

and

$$S_6(h,h_1) = \sum_{0\le h_3<q^{\nu_2-\nu_0}} |\widehat{g}(h_3-h_1-h)\ \widehat{g}(h_3-h_1)\ \widehat{g}(h_3-h)\ \widehat{g}(h_3)|\,.$$

We can majorize $S_6(h,h_1)$ independently of h using the Cauchy–Schwarz inequality,

$$\left(\sum_{0\le h_3<q^{\nu_2-\nu_0}} |\widehat{g}(h_3-h_1-h)\ \widehat{g}(h_3-h)|^2\right)^{1/2} \left(\sum_{0\le h_3<q^{\nu_2-\nu_0}} |\widehat{g}(h_3-h_1)\ \widehat{g}(h_3)|^2\right)^{1/2}.$$

The two quantities in the parentheses above are equal by periodicity, hence

$$S_6(h,h_1) \le S_7(h_1) = \sum_{0\le h'<q^{\nu_2-\nu_0}} |\widehat{g}(h'-h_1)\ \widehat{g}(h')|^2\,. \tag{49}$$

This gives

$$S_5(r,s) \ll q^{2(\nu_2-\nu_0)} \sum_{|h_1|\le H} \left|a_{h_1}(q^{\nu_0-\nu_2},H)\right|^2 S_7(h_1) \sum_{0\le h<q^{\nu_2-\nu_0}} \min\left(q^{\nu}, \left|\sin\pi\frac{2h_1r+2hsq^{\nu_1}}{q^{\nu_2}}\right|^{-1}\right).$$

Intending to sum over s, we observe that the sum above contains terms $2s$, so that it is convenient to extend this sum by adding the terms $2s+1$. Noting by (27), (31), (28), and (42) that $|2h_1rq^{-\nu_1}| \le 2HRq^{-\nu_1} \le \frac{1}{2}$, we can write

$$\frac{1}{S}\sum_{1\le s<S}\sum_{0\le h<q^{\nu_2-\nu_0}} \min\left(q^{\nu}, \left|\sin\pi\frac{2h_1r+(2s)hq^{\nu_1}}{q^{\nu_2}}\right|^{-1}\right)$$
$$\le \frac{2}{2S}\sum_{1\le s'\le 2S}\sum_{0\le h<q^{\nu_2-\nu_0}} \min\left(q^{\nu}, \left|\sin\pi\frac{hs'+2h_1rq^{-\nu_1}}{q^{\nu_2-\nu_1}}\right|^{-1}\right),$$

and observing that the sum over h is $q^{\nu_2-\nu_1}$-periodic, using (16) this is

$$\ll q^{\nu_1-\nu_0}\tau\left(q^{\nu_2-\nu_1}\right)\min\left(q^\nu,\left|\sin\pi\frac{2h_1r}{q^{\nu_2}}\right|^{-1}\right)+q^{\nu_1-\nu_0}q^{\nu_2-\nu_1}\log q^{\nu_2-\nu_1}.$$

Observing by (31), (27), and (42) that $|h_1r|\le HR\le q^{\nu_1}\le q^{\nu_2}/4$, we have

$$q^{\nu_2-\nu_1}\le\min\left(q^\nu,\frac{q^{\nu_2}}{HR}\right)\ll\min\left(q^\nu,\left|\sin\pi\frac{2h_1r}{q^{\nu_2}}\right|^{-1}\right)\le\min\left(q^\nu,\frac{q^{\nu_2}}{r\,|h_1|}\right).$$

Hence

$$\frac{1}{S}\sum_{1\le s<S}S_5(r,s)\ll q^{\nu_1-\nu_0}\left(\tau\left(q^{\nu_2-\nu_1}\right)+\log q^{\nu_2-\nu_1}\right)S_8(r)\tag{50}$$

with

$$S_8(r)=q^{2(\nu_2-\nu_0)}\sum_{|h_1|\le H}\left|a_{h_1}(q^{\nu_0-\nu_2},H)\right|^2S_7(h_1)\min\left(q^\nu,\frac{q^{\nu_2}}{r\,|h_1|}\right).$$

Taking (42) into account, we split the summation $S_8(r)$ in three parts

$$S_8(r)=S_8'(r)+S_8''(r)+S_8'''(r)$$

depending on the size of $|h_1|$: $|h_1|\le q^{2\rho}$, $q^{2\rho}<|h_1|\le q^{\nu_2-\nu_0}$ and $q^{\nu_2-\nu_0}<|h_1|\le H$. Using (10) in $S_8'(r)$, we have $|a_{h_1}(q^{\nu_0-\nu_2},H)|\le\alpha=q^{-(\nu_2-\nu_0)}$, thus

$$\begin{aligned}S_8'(r)&=q^{2(\nu_2-\nu_0)}\sum_{|h_1|\le q^{2\rho}}\left|a_{h_1}(q^{\nu_0-\nu_2},H)\right|^2S_7(h_1)\min\left(q^\nu,\frac{q^{\nu_2}}{r\,|h_1|}\right)\\&\le q^\nu\sum_{|h_1|\le q^{2\rho}}S_7(h_1).\end{aligned}$$

Lemma 9. *If $c>0$ is the constant introduced in Definition 4 and*

$$\nu\le\left(2+\tfrac{4}{3}c\right)\rho,\tag{51}$$

then, uniformly for $\lambda\in\mathbb{N}$ with $\frac{1}{3}(\nu_2-\nu_0)\le\lambda\le\frac{4}{5}(\nu_2-\nu_0)$, we have

$$\sum_{0\le h<q^{\nu_2-\nu_0}}\ \sum_{0\le k<q^{\nu_2-\nu_0-\lambda}}\left|\widehat{g}(h+k)\ \widehat{g}(h)\right|^2\ll_{f,q}q^{\frac{1}{2}(\nu_1-\nu_0)-\frac{1}{2}\gamma(\lambda)}(\log q^{\nu_2-\nu_1})^2.\tag{52}$$

Proof. See [31, Lemma 10]. ☐

By (49) we have

$$\sum_{|h_1|\le q^{2\rho}}S_7(h_1)=\sum_{0\le h'<q^{\nu_2-\nu_0}}\ \sum_{|h_1|\le q^{2\rho}}\left|\widehat{g}(h'-h_1)\ \widehat{g}(h')\right|^2.$$

Applying Lemma 9 with $\lambda=\nu_2-\nu_0-2\rho$ (which by (34), (31), (29), (27), and (33) satisfies $\frac{1}{3}(\nu_2-\nu_0)\le\lambda\le\frac{4}{5}(\nu_2-\nu_0)$, as required in Lemma 9), we get

$$\sum_{|h_1|\le q^{2\rho}}S_7(h_1)\ll_{f,q}q^{\frac{1}{2}(\nu_1-\nu_0)-\frac{1}{2}\gamma(\nu_2-\nu_0-2\rho)}(\log q^{\nu_2-\nu_1})^2,$$

and we obtain

$$S_8'(r)\ll_{f,q}q^{\nu+\frac{1}{2}(\nu_1-\nu_0)-\frac{1}{2}\gamma(\nu_2-\nu_0-2\rho)}(\log q^{\nu_2-\nu_1})^2.$$

Using (10) in $S_8''(r)$, we have $|a_{h_1}(q^{\nu_0-\nu_2},H)| \le \alpha = q^{-(\nu_2-\nu_0)}$, thus

$$\begin{aligned} S_8''(r) &= q^{2(\nu_2-\nu_0)} \sum_{q^{2\rho}<|h_1|\le q^{\nu_2-\nu_0}} \left|a_{h_1}(q^{\nu_0-\nu_2},H)\right|^2 S_7(h_1) \min\left(q^{\nu}, \frac{q^{\nu_2}}{r\,|h_1|}\right) \\ &\le \frac{q^{\nu_2}}{r} \sum_{q^{2\rho}<|h_1|\le q^{\nu_2-\nu_0}} \frac{S_7(h_1)}{|h_1|} \le \frac{q^{\nu_2-2\rho}}{r} \sum_{|h_1|\le q^{\nu_2-\nu_0}} S_7(h_1), \end{aligned}$$

and by (20) and (29) we obtain $S_8''(r) \ll \frac{q^{\nu_2-2\rho}}{r} = \frac{q^{\nu}}{r}$ hence using (28),

$$\frac{1}{R}\sum_{1\le r<R} S_8''(r) \ll q^{\nu}\ \frac{\log R}{R} = \rho\, q^{\nu-\rho}\log q.$$

Using (10) in $S_8'''(r)$, we have $|a_{h_1}(q^{\nu_0-\nu_2},H)| \le \frac{1}{\pi|h_1|}$, thus

$$\begin{aligned} S_8'''(r) &= q^{2(\nu_2-\nu_0)} \sum_{q^{\nu_2-\nu_0}<|h_1|\le H} \left|a_{h_1}(q^{\nu_0-\nu_2},H)\right|^2 S_7(h_1) \min\left(q^{\nu}, \frac{q^{\nu_2}}{r\,|h_1|}\right) \\ &\ll q^{2(\nu_2-\nu_0)}\frac{q^{\nu_2}}{r} \sum_{q^{\nu_2-\nu_0}<|h_1|\le H} \frac{S_7(h_1)}{|h_1|^3}. \end{aligned}$$

Observing that $S_7(h_1)$ is $q^{\nu_2-\nu_0}$ periodic, we split the summation into $jq^{\nu_2-\nu_0} < |h_1| \le (j+1)q^{\nu_2-\nu_0}$, where $1 \le j < H/q^{\nu_2-\nu_0}$, and majorize $|h_1|^{-3}$ by $j^{-3}q^{-3(\nu_2-\nu_0)}$,

$$S_8'''(r) \ll q^{2(\nu_2-\nu_0)}\frac{q^{\nu_2}}{r} \sum_{1\le j<H/q^{\nu_2-\nu_0}} \frac{1}{j^3 q^{3(\nu_2-\nu_0)}} \sum_{0\le h_1<q^{\nu_2-\nu_0}} S_7(h_1),$$

thus by (20), (34), and (31),

$$S_8'''(r) \ll q^{-(\nu_2-\nu_0)}\frac{q^{\nu_2}}{r} = \frac{q^{\nu_0}}{r} \le \frac{q^{\nu-2\rho}}{r}.$$

It follows from the estimates above that

$$\frac{1}{R}\sum_{1\le r<R} S_8(r) \ll_{f,q} q^{\nu+\frac{1}{2}(\nu_1-\nu_0)-\frac{1}{2}\gamma(\nu_2-\nu_0-2\rho)}(\log q^{\nu_2-\nu_1})^2 + \rho\, q^{\nu-\rho}\log q,$$

hence by (50) and (48)

$$\begin{aligned} &\frac{1}{RS}\sum_{1\le r<R}\sum_{1\le s<S} |S_4'(r,s)| \\ &\quad \ll_{f,q} q^{\nu_1-\nu_0}\left(\tau\left(q^{\nu_2-\nu_1}\right) + \log q^{\nu_2-\nu_1}\right) \\ &\qquad \left(q^{\nu+\frac{1}{2}(\nu_1-\nu_0)-\frac{1}{2}\gamma(\nu_2-\nu_0-2\rho)}(\log q^{\nu_2-\nu_1})^2 + \rho\, q^{\nu-\rho}\log q\right). \end{aligned} \tag{53}$$

5.3.2. *Contribution of* $S_4''(r,s)$. We have $h_0 + h_1 \ne 0$, hence the summation over n is an incomplete quadratic Gauss sum. Using (18), we get

$$\begin{aligned} |S_4''(r,s)| \ll & q^{2(\nu_2-\nu_0)} \sum_{|h_0|\le H} \sum_{\substack{|h_1|\le H \\ h_1\ne -h_0}} \left|a_{h_0}(q^{\nu_0-\nu_2},H)\ a_{h_1}(q^{\nu_0-\nu_2},H)\right| \\ & \log(q^{\nu_2})\sqrt{\gcd(h_0+h_1,q^{\nu_2})q^{\nu_2}} \\ & \sum_{0\le h_2<q^{\nu_2-\nu_0}} |\widehat{g}(h_0-h_2)\ \widehat{g}(-h_2)| \sum_{0\le h_3<q^{\nu_2-\nu_0}} |\widehat{g}(h_3-h_1)\ \widehat{g}(h_3)|\,. \end{aligned}$$

By the Cauchy-Schwarz inequality and (20), we have

$$\sum_{0\le h_2<q^{\nu_2-\nu_0}} |\widehat{g}(h_0-h_2)\ \widehat{g}(-h_2)\ | \le 1 \quad\text{and}\quad \sum_{0\le h_3<q^{\nu_2-\nu_0}} |\widehat{g}(h_3-h_1)\ \widehat{g}(h_3)| \le 1,$$

so that

$$|S_4''(r,s)| \ll \log(q^{\nu_2})\ q^{\frac{\nu_2}{2}+2(\nu_2-\nu_0)} \sum_{|h_0|\le H} \sum_{\substack{|h_1|\le H\\ h_1\ne -h_0}} \left|a_{h_0}(q^{\nu_0-\nu_2},H)a_{h_1}(q^{\nu_0-\nu_2},H)\right| \sqrt{\gcd(h_0+h_1,q^{\nu_2})}.$$

Observing that $|h_0+h_1|\le 2H$, we get

$$|S_4''(r,s)| \ll \log(q^{\nu_2})q^{\frac{\nu_2}{2}+2(\nu_2-\nu_0)}H^{1/2} \sum_{|h_0|\le H}\sum_{|h_1|\le H} \left|a_{h_0}(q^{\nu_0-\nu_2},H)a_{h_1}(q^{\nu_0-\nu_2},H)\right|.$$

Furthermore

$$\sum_{|h|\le H} \left|a_h(q^{\nu_0-\nu_2},H)\right| \le \sum_{|h|\le q^{\nu_2-\nu_0}} \frac{1}{q^{\nu_2-\nu_0}} + \sum_{q^{\nu_2-\nu_0}<|h|\le H} \frac{1}{\pi\,|h|} \ll \log(H/q^{\nu_2-\nu_0}) \ll \rho\log q.$$

We deduce that

$$|S_4''(r,s)| \ll \nu_2\rho^2(\log q)^3 q^{\frac{\nu_2}{2}+2(\nu_2-\nu_0)}H^{1/2} \ll (\log q)^3\nu^3 q^{\frac{\nu_2}{2}+2(\nu_2-\nu_0)}H^{1/2}. \tag{54}$$

5.3.3. *Conclusion.* From (53) and (54) we conclude that

$$\begin{aligned}\frac{1}{RS}\sum_{1\le r<R}\sum_{1\le s<S} S_4(r,s) &\ll_{f,q} q^{\nu_1-\nu_0}\left(\tau\left(q^{\nu_2-\nu_1}\right)+\log q^{\nu_2-\nu_1}\right)\\ &\qquad \left(q^{\nu+\frac12(\nu_1-\nu_0)-\frac12\gamma(\nu_2-\nu_0-2\rho)}(\log q^{\nu_2-\nu_1})^2+\rho\, q^{\nu-\rho}\log q\right)\\ &\quad + (\log q)^3\nu^3 q^{\frac{\nu_2}{2}+2(\nu_2-\nu_0)}H^{1/2},\end{aligned}$$

hence, by (45), (37), (36), (29), (31), (34), (27), and (42) we obtain

$$\begin{aligned}|S_0|^4 \ll_{f,q} & \ q^{4\nu-\rho}+q^{4\nu-2\rho'}\\ &+\left(\tau\left(q^{4\rho}\right)+\log q^{4\rho}\right)\left(q^{4\nu+3\rho'-\frac12\gamma(2\rho+2\rho')}(\log q^{4\rho})^2+\rho\, q^{4\nu+2\rho'-\rho}\log q\right)\\ &+(\log q)^3\nu^3 q^{\frac{7\nu}{2}+\rho+2(4\rho+2\rho')+3\rho+\rho'},\end{aligned}$$

which, using $\tau\left(q^{4\rho}\right) \ll (4\rho)^{\omega(q)}\tau(q)$ (by multiplicativity), the fact that γ is nondecreasing and choosing

$$\rho' = \lfloor \gamma(2\rho)/7\rfloor, \tag{55}$$

by (21) we have $\rho'\le\rho/7$, and we get

$$|S_0|^4 \quad \ll_{f,q} \quad \rho^{\omega(q)+2}q^{4\nu-\frac{\gamma(2\rho)}{14}}+\nu^3 q^{\frac{7\nu}{2}+12\rho+5\frac{\rho}{7}}.$$

Choosing

$$\rho = \lfloor 7\nu/179\rfloor, \tag{56}$$

in order to ensure (51), it is sufficient to check that

$$\nu \leq \left(2+\tfrac{4}{3}c\right)\left(\frac{7\nu}{179}-1\right),$$

which is true for ν large enough and

$$c \geq c_0 = 18. \tag{57}$$

This gives

$$|S_0|^4 \quad \ll_{f,q} \quad \nu^{\omega(q)+2}\left(q^{4\nu-\frac{\gamma(2\lfloor 7\nu/179\rfloor)}{14}} + q^{4\nu-\frac{\nu}{358}}\right),$$

and using again (21) this establish (26).

6. Proof of Theorem 1

We apply (26) with N replaced by $\lfloor x/q^k \rfloor$, and we sum over k. Let $K \in \mathbb{N}$ such that $q^K \leq x^{163/700} < q^{K+1}$. Since γ is nondecreasing, we have

$$\begin{aligned}\sum_{k\leq K} \frac{x}{q^k} q^{-\gamma\left(2\left\lfloor (7\log(xq^{-k}))/(179\log q)\right\rfloor\right)/56} &\leq q^{-\gamma(2\lfloor (3\log x)/(100\log q)\rfloor)/56} \sum_{k\leq K}\frac{x}{q^k}\\ &\leq x\, q^{-\gamma(2\lfloor (3\log x)/(100\log q)\rfloor)/56},\end{aligned}$$

while

$$\begin{aligned}\sum_{k>K} \frac{x}{q^k} q^{-\gamma\left(2\left\lfloor 7\log(xq^{-k})/179\log q\right\rfloor\right)/56} &\leq \sum_{k>K}\frac{x^{537/700}}{q^k} \ll x^{537/700}\\ &\ll x\, q^{-\gamma(2\lfloor 3\log x/100\log q\rfloor)/56},\end{aligned}$$

which establish (4) and complete the proof of Theorem 1.

7. Application to Rudin–Shapiro sequences

7.1. **Rudin–Shapiro sequences of order δ.** We proved in [31, Section 10.1] that any Rudin–Shapiro sequence of order δ verifies Definition 3 and belongs to $\mathcal{F}_{\gamma,c}$ in Definition 4 for any $c > 0$ and

$$\gamma(\lambda) = -\frac{\lambda}{2\log 2}\log\left(\frac{1+|\cos\pi\alpha|}{2}\right) - \frac{\delta+1}{2}. \tag{58}$$

Applying Theorem 1, we obtain

Theorem 2. *For any $\delta \in \mathbb{N}$, $\alpha \in \mathbb{R}$, $\vartheta \in \mathbb{R}$, and $x \geq 2$, we have*

$$\left|\sum_{n\leq x} r_\delta(n^2,\alpha)\,\mathrm{e}(\vartheta n)\right| \ll x\,(\log x)^3\, 2^{-\frac{\gamma(2\lfloor (7\log x)/(179\log 2)\rfloor)}{14}}, \tag{59}$$

where γ is defined by (58)*.*

If $(\beta_\delta(n))_{n\in\mathbb{N}}$ is the sequence defined for any $n \in \mathbb{N}$ by

$$\beta_\delta(n) = \sum_{k\geq\delta+1} \varepsilon_{k-\delta-1}(n)\,\varepsilon_k(n),$$

then the following corollaries can be easily deduced from Theorem 2.

Corollary 1. *The sequence $(\alpha\beta_\delta(n^2))_{n\in\mathbb{N}}$ is uniformly distributed modulo 1 if and only if $\alpha \in \mathbb{R}\setminus\mathbb{Q}$.*

Proof. If $\alpha \in \mathbb{Q}$, then the sequence $(\alpha\beta_\delta(n^2))_{n\in\mathbb{N}}$ takes only a finite number of different values, thus it is not uniformly distributed modulo 1. If $\alpha \in \mathbb{R}\setminus\mathbb{Q}$, then for all $h \in \mathbb{Z}$ such that $h \neq 0$, it follows from Theorem 2 that there exists $\sigma_2(h\alpha) > 0$ such that

$$\sum_{n\le x} \mathrm{e}(h\alpha\beta_\delta(n^2)) = \sum_{n\le x} r_\delta(n^2, h\alpha) = O(x^{1-\sigma_2(h\alpha)}).$$

By the Weyl criterion [34, chapter 1, p. 1] this shows the uniform distribution modulo 1 of the sequence $(\alpha\beta_\delta(n^2))_{n\in\mathbb{N}}$. □

Corollary 2. *For any $m \in \mathbb{N}$, $m \geq 2$, there exists $\sigma_m > 0$ such that for any $a \in \mathbb{Z}$, we have*

$$\mathrm{card}\{n \le x,\ \beta_\delta(n^2) \equiv a \bmod m\} = \frac{x}{m} + O_m(x^{1-\sigma_m}). \tag{60}$$

Proof. We have

$$\begin{aligned}\mathrm{card}\{n \le x,\ \beta_\delta(n^2) \equiv a \bmod m\} &= \sum_{n\le x} \frac{1}{m} \sum_{0\le j<m} \mathrm{e}\left(\frac{j}{m}(\beta_\delta(n^2) - a)\right)\\ &= \frac{x}{m} + \frac{1}{m} \sum_{1\le j<m} \mathrm{e}\left(\frac{-ja}{m}\right) \sum_{n\le x} \mathrm{e}\left(\frac{j}{m}\beta_\delta(n^2)\right).\end{aligned}$$

By Theorem 2, for any $j \in \{1, \ldots, m-1\}$, there exists $\sigma(j,m) > 0$ such that

$$\sum_{n\le x} \mathrm{e}\left(\frac{j}{m}\beta_\delta(n^2)\right) = O(x^{1-\sigma(j,m)}).$$

Taking $\sigma_m = \min_{1\le j<m} \sigma(j,m) > 0$, we obtain (60). □

By similar arguments we can prove

Corollary 3. *For any $(m,a) \in \mathbb{N}\times\mathbb{Z}$, $m \geq 2$, the sequence $(\vartheta n)_{n\in\mathbb{N},\ \beta_\delta(n^2)\equiv a \bmod m}$ is uniformly distributed modulo 1 if and only if $\vartheta \in \mathbb{R}\setminus\mathbb{Q}$.*

7.2. **Rudin–Shapiro sequences of degree d.** We proved in [31, Section 10.2] that any Rudin–Shapiro sequence of degree d verifies Definition 3 and belongs to $\mathcal{F}_{\gamma,c}$ in Definition 4 for any $c > 0$ and

$$\gamma(\lambda) = \frac{-\lambda}{d\ \log 2} \log\left(1 - 2^{3-d}\left(\sin\tfrac{\pi\|\alpha\|}{4}\right)^2\right) - \frac{1}{2}. \tag{61}$$

Applying Theorem 1, we obtain

Theorem 3. *For any $d \in \mathbb{N}$ with $d \geq 2$, $\alpha \in \mathbb{R}$, $\vartheta \in \mathbb{R}$, and $x \geq 2$, we have*

$$\left|\sum_{n\le x} R_d(n^2,\alpha)\,\mathrm{e}(\vartheta n)\right| \ll x\,(\log x)^3\, 2^{-\frac{\gamma(2\lfloor(7\log x)/(179\log 2)\rfloor)}{14}}, \tag{62}$$

where γ is defined by (61).

If $(b_d(n))_{n\in\mathbb{N}}$ is the sequence defined for any $n \in \mathbb{N}$ by

$$b_d(n) = \sum_{k\ge d-1} \varepsilon_{k-d+1}(n)\cdots\varepsilon_k(n),$$

by arguments similar to section 7.1 the following corollaries can be deduced from Theorem 3.

Corollary 4. *The sequence* $(\alpha b_d(n^2))_{n\in\mathbb{N}}$ *is uniformly distributed modulo* 1 *if and only if* $\alpha \in \mathbb{R}\setminus\mathbb{Q}$.

Corollary 5. *For any* $m \in \mathbb{N}$, $m \geq 2$, *there exists* $\sigma_m > 0$ *such that for any* $a \in \mathbb{Z}$, *we have*

$$\mathrm{card}\{n \leq x,\ b_d(n^2) \equiv a \bmod m\} = \frac{x}{m} + O_m(x^{1-\sigma_m}).$$

Corollary 6. *For any* $(m,a) \in \mathbb{N}\times\mathbb{Z}$, $m \geq 2$, *the sequence* $(\vartheta n)_{n\in\mathbb{N},\ b_d(n^2)\equiv a \bmod m}$ *is uniformly distributed modulo* 1 *if and only if* $\vartheta \in \mathbb{R}\setminus\mathbb{Q}$.

References

[1] J.-P. Allouche and P. Liardet, *Generalized Rudin-Shapiro sequences*, Acta Arith. **60** (1991), no. 1, 1–27. MR1129977

[2] J.-P. Allouche and M. Mendès France, *On an extremal property of the Rudin-Shapiro sequence*, Mathematika **32** (1985), no. 1, 33–38, DOI 10.1112/S0025579300010822. MR817104

[3] J.-P. Allouche and M. Mendès France, *Suite de Rudin-Shapiro et modèle d'Ising* (French, with English summary), Bull. Soc. Math. France **113** (1985), no. 3, 273–283. MR834040

[4] N. L. Bassily and I. Kátai, *Distribution of the values of q-additive functions on polynomial sequences*, Acta Math. Hungar. **68** (1995), no. 4, 353–361, DOI 10.1007/BF01874349. MR1333478

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

[6] V. Bergelson and A. Leibman, *Polynomial extensions of van der Waerden's and Szemerédi's theorems*, J. Amer. Math. Soc. **9** (1996), no. 3, 725–753, DOI 10.1090/S0894-0347-96-00194-4. MR1325795

[7] J. Bourgain, *On the maximal ergodic theorem for certain subsets of the integers*, Israel J. Math. **61** (1988), no. 1, 39–72, DOI 10.1007/BF02776301. MR937581

[8] J. Bourgain, *On the pointwise ergodic theorem on* L^p *for arithmetic sets*, Israel J. Math. **61** (1988), no. 1, 73–84, DOI 10.1007/BF02776302. MR937582

[9] J. Bourgain, *Pointwise ergodic theorems for arithmetic sets*, Inst. Hautes Études Sci. Publ. Math. **69** (1989), 5–45. With an appendix by the author, Harry Furstenberg, Yitzhak Katznelson and Donald S. Ornstein. MR1019960

[10] J. Brillhart and L. Carlitz, *Note on the Shapiro polynomials*, Proc. Amer. Math. Soc. **25** (1970), 114–118, DOI 10.2307/2036537. MR0260955

[11] J. Brillhart and P. Morton, *Über Summen von Rudin-Shapiroschen Koeffizienten* (German, with English summary), Illinois J. Math. **22** (1978), no. 1, 126–148. MR0476686

[12] J. R. Büchi, *Weak second-order arithmetic and finite automata*, Z. Math. Logik Grundlagen Math. **6** (1960), 66–92. MR0125010

[13] Z. Buczolich and R. D. Mauldin, *Divergent square averages*, Ann. of Math. (2) **171** (2010), no. 3, 1479–1530, DOI 10.4007/annals.2010.171.1479. MR2680392

[14] A. Cobham, *Uniform tag sequences*, Math. Systems Theory **6** (1972), 164–192, DOI 10.1007/BF01706087. MR0457011

[15] A. Connes and E. J. Woods, *Approximately transitive flows and ITPFI factors*, Ergodic Theory Dynam. Systems **5** (1985), no. 2, 203–236, DOI 10.1017/S0143385700002868. MR796751

[16] H. Davenport and P. Erdős, *Note on normal decimals*, Canadian J. Math. **4** (1952), 58–63. MR0047084

[17] M. Drmota, C. Mauduit, and J. Rivat, *The sum-of-digits function of polynomial sequences*, J. Lond. Math. Soc. (2) **84** (2011), no. 1, 81–102, DOI 10.1112/jlms/jdr003. MR2819691

[18] M. Drmota and J. F. Morgenbesser, *Generalized Thue-Morse sequences of squares*, Israel J. Math. **190** (2012), 157–193, DOI 10.1007/s11856-011-0186-2. MR2956237

[19] E. H. El Abdalaoui and M. Lemańczyk, *Approximate transitivity property and Lebesgue spectrum*, Monatsh. Math. **161** (2010), no. 2, 121–144, DOI 10.1007/s00605-010-0223-y. MR2680002

[20] N. P. Frank, *Substitution sequences in* $\mathbb{Z}^d$ *with a non-simple Lebesgue component in the spectrum*, Ergodic Theory Dynam. Systems **23** (2003), no. 2, 519–532, DOI 10.1017/S0143385702001256. MR1972236

[21] H. Furstenberg, *Problem session*, Conference on Ergodic Theory and Applications, University of New Hampshire, Durham, NH, June 1982, (1982).

[22] B. Host and B. Kra, *Convergence of polynomial ergodic averages*, Israel J. Math. **149** (2005), 1–19, DOI 10.1007/BF02772534. Probability in mathematics. MR2191208

[23] B. Host and B. Kra, *Nonconventional ergodic averages and nilmanifolds*, Ann. of Math. (2) **161** (2005), no. 1, 397–488, DOI 10.4007/annals.2005.161.397. MR2150389

[24] J.-P. Kahane, *Hélices et quasi-hélices* (French), Mathematical analysis and applications, Part B, Adv. in Math. Suppl. Stud., vol. 7, Academic Press, New York-London, 1981, pp. 417–433. MR634251

[25] J.-P. Kahane and R. Salem, *Ensembles parfaits et séries trigonométriques* (French, with French summary), 2nd ed., Hermann, Paris, 1994. With notes by Kahane, Thomas W. Körner, Russell Lyons and Stephen William Drury. MR1303593

[26] T. Kamae and M. Keane, *A class of deterministic self-affine processes*, Japan J. Appl. Math. **7** (1990), no. 2, 183–195, DOI 10.1007/BF03167840. MR1057528

[27] M. Lemańczyk, *Toeplitz Z_2-extensions* (English, with French summary), Ann. Inst. H. Poincaré Probab. Statist. **24** (1988), no. 1, 1–43. MR937955

[28] J. Mathew and M. G. Nadkarni, *A measure preserving transformation whose spectrum has Lebesgue component of multiplicity two*, Bull. London Math. Soc. **16** (1984), no. 4, 402–406, DOI 10.1112/blms/16.4.402. MR749448

[29] C. Mauduit and J. Rivat, *La somme des chiffres des carrés* (French), Acta Math. **203** (2009), no. 1, 107–148, DOI 10.1007/s11511-009-0040-0. MR2545827

[30] C. Mauduit and J. Rivat, *Sur un problème de Gelfond: la somme des chiffres des nombres premiers* (French, with English and French summaries), Ann. of Math. (2) **171** (2010), no. 3, 1591–1646, DOI 10.4007/annals.2010.171.1591. MR2680394

[31] C. Mauduit and J. Rivat, *Prime numbers along Rudin-Shapiro sequences*, J. Eur. Math. Soc. (JEMS) **17** (2015), no. 10, 2595–2642, DOI 10.4171/JEMS/566. MR3420517

[32] M. Mendès France and G. Tenenbaum, *Dimension des courbes planes, papiers pliés et suites de Rudin-Shapiro* (French, with English summary), Bull. Soc. Math. France **109** (1981), no. 2, 207–215. MR623789

[33] M. Minsky and S. Papert, *Unrecognizable sets of numbers*, J. Assoc. Comput. Mach. **13** (1966), 281–286, DOI 10.1145/321328.321337. MR0207481

[34] H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, CBMS Regional Conference Series in Mathematics, vol. 84, Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1994. MR1297543

[35] M. Peter, *The summatory function of the sum-of-digits function on polynomial sequences*, Acta Arith. **104** (2002), no. 1, 85–96, DOI 10.4064/aa104-1-4. MR1913736

[36] N. P. Fogg, *Substitutions in dynamics, arithmetics and combinatorics*, Lecture Notes in Mathematics, vol. 1794, Springer-Verlag, Berlin, 2002. Edited by V. Berthé, S. Ferenczi, C. Mauduit and A. Siegel. MR1970385

[37] M. Queffélec, *Substitution dynamical systems—spectral analysis*, Lecture Notes in Mathematics, vol. 1294, Springer-Verlag, Berlin, 1987. MR924156

[38] M. Queffélec, *Une nouvelle propriété des suites de Rudin-Shapiro* (French, with English summary), Ann. Inst. Fourier (Grenoble) **37** (1987), no. 2, 115–138. MR898934

[39] R. W. Ritchie, *Finite automata and the set of squares*, J. Assoc. Comput. Mach. **10** (1963), 528–531, DOI 10.1145/321186.321196. MR0167374

[40] W. Rudin, *Some theorems on Fourier coefficients*, Proc. Amer. Math. Soc. **10** (1959), 855–859, DOI 10.2307/2033608. MR0116184

[41] B. Saffari, *Une fonction extrémale liée à la suite de Rudin-Shapiro* (French, with English summary), C. R. Acad. Sci. Paris Sér. I Math. **303** (1986), no. 4, 97–100. MR853595

[42] H. S. Shapiro, *Extremal problems for polynomials and power series.* M.S. Thesis, M.I.T., 1951.

[43] J. D. Vaaler, *Some extremal functions in Fourier analysis*, Bull. Amer. Math. Soc. (N.S.) **12** (1985), no. 2, 183–216, DOI 10.1090/S0273-0979-1985-15349-2. MR776471

Université d'Aix-Marseille et Institut Universitaire de France, Institut de Mathématiques de Marseille, CNRS UMR 7373, Case 907, 163, avenue de Luminy, 13288 MARSEILLE Cedex 9, France
Email address: mauduit@iml.univ-mrs.fr

Université d'Aix-Marseille, Institut de Mathématiques de Marseille, CNRS UMR 7373, Case 907, 163, avenue de Luminy, 13288 MARSEILLE Cedex 9, France
Email address: joel.rivat@univ-amu.fr