Lukas SPIEGELHOFER

_Pseudorandomness of the Ostrowski sum-of-digits function_

<http://jtnb.cedram.org/item?id=JTNB_2018__30_2_637_0>
Pseudorandomness of the Ostrowski sum-of-digits function

par Lukas SPIEGELHOFER

Résumé. Pour un nombre irrationnel $\alpha \in (0, 1)$, nous étudions la fonction somme des chiffres d’Ostrowski $\sigma_\alpha$. Étant donné un nombre $\alpha$ à quotients partiels bornés et un nombre $\vartheta \in \mathbb{R} \setminus \mathbb{Z}$, nous montrons que la fonction $g : n \mapsto e(\vartheta \sigma_\alpha(n))$, où $e(x) = e^{2\pi ix}$, est pseudo-aléatoire dans le sens suivant : pour tout $r \in \mathbb{N}$ la limite

$$\gamma_r = \lim_{N \to \infty} \frac{1}{N} \sum_{0 \leq n < N} g(n + r)\overline{g(n)}$$

existe et on a

$$\lim_{R \to \infty} \frac{1}{R} \sum_{0 \leq r < R} |\gamma_r|^2 = 0.$$ 

Abstract. For an irrational $\alpha \in (0, 1)$, we investigate the Ostrowski sum-of-digits function $\sigma_\alpha$. For $\alpha$ having bounded partial quotients and $\vartheta \in \mathbb{R} \setminus \mathbb{Z}$, we prove that the function $g : n \mapsto e(\vartheta \sigma_\alpha(n))$, where $e(x) = e^{2\pi ix}$, is pseudorandom in the following sense: for all $r \in \mathbb{N}$ the limit

$$\gamma_r = \lim_{N \to \infty} \frac{1}{N} \sum_{0 \leq n < N} g(n + r)\overline{g(n)}$$

exists and we have

$$\lim_{R \to \infty} \frac{1}{R} \sum_{0 \leq r < R} |\gamma_r|^2 = 0.$$ 


2010 Mathematics Subject Classification. 11A55, 11A67.


The author acknowledges support by the Austrian Science Fund (FWF), project F5505-N26, which is a part of the Special Research Program “Quasi Monte Carlo Methods: Theory and Applications”, and by the project MuDeRa (Multiplicativity, Determinism and Randomness), which is a joint project between the ANR (Agence Nationale de la Recherche) and the FWF (Austrian Science Fund, grant I-1751-N26).
1. Introduction and main results

Let $g$ be an arithmetical function. The set of $\beta \in [0, 1)$ satisfying

$$
\limsup_{N \to \infty} \frac{1}{N} \left| \sum_{0 \leq n < N} g(n) e(-n\beta) \right| > 0
$$

is called the Fourier–Bohr spectrum of $g$.

The function $g$ is called pseudorandom in the sense of Bertrandias [4] or simply pseudorandom if the limit

$$
\gamma_r = \lim_{N \to \infty} \frac{1}{N} \sum_{0 \leq n < N} g(n + r) \overline{g(n)}
$$

exists for all $r \geq 0$ and is zero in quadratic mean, that is,

$$
\lim_{R \to \infty} \frac{1}{R} \sum_{0 \leq r < R} |\gamma_r|^2 = 0.
$$

Pseudorandomness can be understood as a property of the spectral measure associated to $g$: Assume that the correlation $\gamma_r$ of $g$ exists for all $r \geq 0$. By the Bochner representation theorem there exists a unique measure $\mu$ on the Torus $T = \mathbb{R}/\mathbb{Z}$ such that

$$
\gamma_r = \int_T e(rx) \, d\mu(x)
$$

for all $r$. Then $g$ is pseudorandom if and only if the discrete component of $\mu$ vanishes. We refer to [9] for more details.

It is known that pseudorandomness of a bounded arithmetic function $g$ implies that the spectrum of $g$ is empty, which can be proved using van der Corput’s inequality. For the convenience of the reader, we give a proof of this fact in Section 2.

The converse of this statement does not always hold. However, it is true for $q$-multiplicative functions $g : \mathbb{N} \to T = \{z \in \mathbb{C} : |z| = 1\}$, which has been proved by Coquet [5, 6, 7]. Here a function $g : \mathbb{N} \to \mathbb{C}$ is called $q$-multiplicative if $f(q^k n + b) = f(q^k n) f(b)$ for all integers $k, n > 0$ and $0 \leq b < q^k$.

The purpose of this paper is to prove an analogous statement for the Ostrowski numeration system, that is, for $\alpha$-multiplicative functions. Assume that $\alpha \in (0, 1)$ is irrational. The Ostrowski numeration system has as its scale of numeration the sequence of denominators of the convergents of the regular continued fraction expansion of $\alpha$. More precisely, let $\alpha = [0; a_1, a_2, \ldots]$ be the continued fraction expansion of $\alpha$ and $p_i/q_i =$
[0; a_1, \ldots, a_i] the i-th convergent to \( \alpha \), where \( i \geq 0 \). By the greedy algorithm, every nonnegative integer \( n \) has a representation

\[
(1.1) \quad n = \sum_{k \geq 0} \varepsilon_k q_k
\]

such that

\[
\sum_{0 \leq k < K} \varepsilon_k q_k < qK
\]

for all \( K \geq 0 \). This algorithm yields the unique expansion of the form (1.1) having the properties that \( 0 \leq \varepsilon_0 < a_1, 0 \leq \varepsilon_k \leq a_{k+1} \) and \( \varepsilon_k = a_{k+1} \Rightarrow \varepsilon_{k-1} = 0 \) for \( k \geq 1 \), the Ostrowski expansion of \( n \).

For a nonnegative integer \( n \) let \( (\varepsilon_k(n))_{k \geq 0} \) be its Ostrowski expansion. An arithmetic function \( f \) is \( \alpha \)-additive resp. \( \alpha \)-multiplicative if

\[
f(n) = \sum_{k \geq 0} f(\varepsilon_k(n) q_k) \quad \text{resp.} \quad f(n) = \prod_{k \geq 0} f(\varepsilon_k(n) q_k)
\]

for all \( n \). Examples of \( \alpha \)-additive functions are the functions \( n \mapsto \beta n \) (for \( \beta \in \mathbb{R} \)) and the \( \alpha \)-sum of digits of \( n \) [8]:

\[
\sigma_\alpha(n) = \sum_{i \geq 0} \varepsilon_i(n).
\]

We refer the reader to [3] for a survey on the Ostrowski numeration system. In particular, we want to note that the Ostrowski numeration system is a useful tool for studying the discrepancy modulo 1 of \( n\alpha \)-sequences, see for example the references contained in the aforementioned paper.

Moreover, see [2] for a dynamical viewpoint of the Ostrowski numeration system, see also [1, 12] for more general numeration systems.

Our main theorem establishes a connection between the Fourier–Bohr spectrum and pseudorandomness for \( \alpha \)-multiplicative functions.

**Theorem 1.1.** Assume that \( g \) is a bounded \( \alpha \)-multiplicative function. The Fourier–Bohr spectrum of \( g \) is empty if and only if \( g \) is pseudorandom.

Using a theorem by Coquet, Rhin and Toffin [11, Theorem 2], we obtain the following corollary.

**Corollary 1.2.** Assume that \( \alpha \in (0, 1) \) is irrational and has bounded partial quotients and \( \vartheta \in \mathbb{R} \setminus \mathbb{Z} \). Then \( n \mapsto e(\vartheta \sigma_\alpha(n)) \) is pseudorandom.

In particular, this holds for the Zeckendorf sum-of-digits function, which corresponds to the case \( \alpha = (\sqrt{5} - 1)/2 = [0; 1, 1, \ldots] \). This special case can be found in the author’s thesis [14].

We first present a series of auxiliary results, and proceed to the proof of Theorem 1.1 in Section 3.
2. Lemmas

We begin with the well-known inequality of van der Corput.

**Lemma 2.1** (Van der Corput’s inequality). Let $I$ be a finite interval in $\mathbb{Z}$ and let $a_n \in \mathbb{C}$ for $n \in I$. Then

$$\left| \sum_{n \in I} a_n \right|^2 \leq \frac{|I| - 1 + R}{R} \sum_{0 \leq |r| < R} \left( 1 - \frac{|r|}{R} \right) \sum_{n \in I, n+r \in I} a_{n+r} \overline{a_n}$$

for all integers $R \geq 1$.

In the definition of pseudorandomness for bounded arithmetic functions $g$, we do not actually need the square.

**Lemma 2.2.** Let $g$ be a bounded arithmetic function such that the correlation $\gamma_r$ of $g$ exists for all $r \geq 0$. The function $g$ is pseudorandom if and only if

$$\lim_{R \to \infty} \frac{1}{R} \sum_{0 \leq r < R} |\gamma_r| = 0.$$

For the proof of sufficiency we note that we may without loss of generality assume that $|g| \leq 1$. The other direction is an application of the Cauchy-Schwarz inequality.

As we noted before, pseudorandomness of $g$ implies that the spectrum of $g$ is empty.

**Lemma 2.3.** Let $g$ be a bounded arithmetic function. If $g$ is pseudorandom, then the Fourier–Bohr spectrum of $g$ is empty.

**Proof.** The proof is an application of van der Corput’s inequality (Lemma 2.1). We have for all $R \in \{1, \ldots, N\}$

$$\left| \frac{1}{N} \sum_{0 \leq n < N} g(n) e(n\beta) \right|^2 \leq \frac{N - 1 + R}{RN^2} \sum_{0 \leq |r| < R} \left( 1 - \frac{|r|}{R} \right) e(r\beta) \sum_{0 \leq n, n+r < N} g(n+r) \overline{g(n)}$$

$$\ll \frac{1}{R} \sum_{0 \leq r < R} \left| \frac{1}{N} \sum_{0 \leq n < N} g(n+r) \overline{g(n)} \right| + O\left( \frac{R}{N} \right).$$

Let $\varepsilon \in (0, 1)$. By hypothesis and Lemma 2.2 we may choose $R$ so large that

$$\frac{1}{R} \sum_{0 \leq r < R} |\gamma_r| < \varepsilon^2.$$
Moreover, we choose $N_0$ in such a way that $R/N_0 < \varepsilon^2$ and

$$\frac{1}{N} \left| \sum_{0 \leq n < N} g(n + r)\overline{g(n)} - \gamma_r \right| < \varepsilon^2$$

for all $r < R$ and $N \geq N_0$. Then for $N \geq N_0$ we have

$$\left| \frac{1}{N} \sum_{0 \leq n < N} g(n) e(n\beta) \right|^2 \leq \frac{1}{R} \sum_{0 \leq r < R} \left| \frac{1}{N} \sum_{0 \leq n < N} g(n + r)\overline{g(n)} - \gamma_r \right| + \frac{1}{R} \sum_{0 \leq r < R} |\gamma_r| + O\left(\frac{R}{N_0}\right)$$

$$\leq \varepsilon^2. \quad \square$$

The following lemma is a generalization of Dini’s Theorem.

**Lemma 2.4.** Assume that $(f_i)_{i \geq 0}$ is a sequence of nonnegative continuous functions on $[0, 1]$ converging pointwise to the zero function. Assume that $|f_{i+1}(x)| \leq \max\{|f_i(x)|, |f_{i-1}(x)|\}$ for $x \in [0, 1]$. Then the convergence is uniform in $x$.

**Proof.** For $\varepsilon > 0$ and nonnegative $N$ we set

$$A_N(\varepsilon) = \{x \in [0, 1] : f_N(x) < \varepsilon \text{ and } f_{N+1}(x) < \varepsilon\}.$$

Note that this is an open set. By induction, using the property $|f_{i+1}(x)| \leq \max\{|f_i(x)|, |f_{i-1}(x)|\}$, we obtain

$$A_N(\varepsilon) = \{x \in [0, 1] : f_n(x) < \varepsilon \text{ for all } n \geq N\}.$$

Trivially, we have $A_N(\varepsilon) \subseteq A_{N+1}(\varepsilon)$. For each $x \in [0, 1]$ there is an $N(x)$ such that $f_n(x) < \varepsilon$ for all $n \geq N(x)$. Then $x \in A_{N(x)}(\varepsilon)$, therefore $(A_{N(x)}(\varepsilon))_{x \in [0, 1]}$ is an open cover of the compact set $[0, 1]$. Choose $x_1, \ldots, x_k$ such that $A_{N(x_1)}(\varepsilon) \cup \cdots \cup A_{N(x_k)}(\varepsilon) \supseteq [0, 1]$ and set $N = \max\{N(x_1), \ldots, N(x_k)\}$. By monotonicity of the sets $A_N(\varepsilon)$, we obtain $A_N(\varepsilon) \supseteq [0, 1]$, in other words, $f_n(x) < \varepsilon$ for all $x \in [0, 1]$ and all $n \geq N$. \square

**Lemma 2.5.** Assume that $\lambda \geq 1$ and let $(w_i)_i$ be the increasing enumeration of the integers $n$ such that $\varepsilon_0(n) = \cdots = \varepsilon_{\lambda-1}(n) = 0$. The intervals $[w_i, w_{i+1})$ constitute a partition of the set $\mathbb{N}$ into intervals of length $q_\lambda$ and $q_{\lambda-1}$, where $w_{i+1} - w_i = q_{\lambda-1}$ if and only if $\varepsilon_\lambda(w_i) = a_{\lambda+1}$.

**Proof.** Assume first that $\varepsilon_\lambda(w_i) = a_{\lambda+1}$. We want to show that $w_{i+1} = w_i + q_{\lambda-1}$. Assume that $\lambda \geq 2$ and let $w_i \leq n < w_i + q_{\lambda-1}$. Then the Ostrowski expansion of $n$ is obtained by superposition of the expansions of $w_i$ and of $n - w_i$. In particular, for $w_i < n < w_i + q_{\lambda-1}$ we have $\varepsilon_j(n) \neq 0$
for some \( j < \lambda - 1 \). (Trivially, this also holds for \( \lambda = 1 \).) Moreover, in the addition \( w_i + q_{\lambda-1} \) a carry occurs, producing \( \varepsilon_j(w_i + q_{\lambda-1}) = 0 \) for \( j \leq \lambda \), therefore \( w_{i+1} = w_i + q_{\lambda-1} \). The case \( \varepsilon_\lambda(w_i) < a_{\lambda+1} \) is similar, in which case \( w_{i+1} = w_i + q_\lambda \). \( \square \)

For an \( \alpha \)-multiplicative function \( g \) and an integer \( \lambda \geq 0 \) we define a function \( g_\lambda \) by truncating the digital expansion: we define \( \psi_\lambda(n) = \sum_{i<\lambda} \varepsilon_i(n)q_i \) and

\[
g_\lambda(n) = g(\psi_\lambda(n)).
\]

We will need the following carry propagation lemma for the Ostrowski numeration system.

**Lemma 2.6.** Let \( \lambda \geq 1 \) be an integer and \( N, r \geq 0 \). Assume that \( \alpha \in (0,1) \) is irrational and let \( g \) be an \( \alpha \)-multiplicative function. Then

\[
(2.1) \quad \left| \left\{ n < N : g(n + r)g(n) \neq g_\lambda(n + r)g_\lambda(n) \right\} \right| \leq N \frac{r}{q_{\lambda-1}}.
\]

**Proof.** The statement we want to prove is trivial for \( r \geq q_{\lambda-1} \), we assume therefore that \( r < q_{\lambda-1} \). Let \( w \) be the family from Lemma 2.5. For \( w_i \leq n < w_{i+1} - r \), we have \( \varepsilon_j(n + r) = \varepsilon_j(n) \) for \( j \geq \lambda \). It follows that

\[
\left| \left\{ n \in \{w_i, \ldots, w_{i+1} - 1\} : g(n + r)g(n) \neq g_\lambda(n + r)g_\lambda(n) \right\} \right| \leq r.
\]

By concatenating blocks, the statement follows therefore for the case that \( N = w_i \) for some \( i \). It remains to treat the case that \( w_i < N < w_{i+1} \) for some \( i \). To this end, we denote by \( L(N) \) resp. \( R(N) \) the left hand side resp. the right hand side of (2.1). For \( w_i \leq N \leq w_{i+1} \) we have

\[
L(N) = \begin{cases} L(w_i), & N \leq w_{i+1} - r; \\ L(w_i) + N - (w_{i+1} - r), & N \geq w_{i+1} - r. \end{cases}
\]

Note that \( L \) is a polygonal line that lies below \( R(N) \) for \( N \in \{w_i, w_{i+1} - r, w_{i+1}\} \) and therefore for all \( N \in \{w_i, w_{i+1}\} \). By concatenating blocks, the full statement follows. \( \square \)

We define Fourier coefficients for \( g \):

\[
G_\lambda(h) = \frac{1}{q_\lambda} \sum_{0 \leq u < q_\lambda} g(u) e(-huq_\lambda^{-1}).
\]

**Lemma 2.7.** Assume that \( i \) is such that \( w_{i+1} - w_i = q_\lambda \) and let \( r \geq 0 \). We have

\[
(2.2) \quad \sum_{h < q_\lambda} |G_\lambda(h)|^2 e(hrq_\lambda^{-1}) = \frac{1}{q_\lambda} \sum_{w_i \leq v < w_{i+1}} g_\lambda(v + r)g_\lambda(v) + O\left( \frac{r}{q_\lambda} \right).
\]
Proof.

\[
\sum_{0 \leq h < q} |G_{\lambda}(h)|^2 e(hrq^{-1})
\]

\[= q^{-1} \sum_{0 \leq u, v < q} g_{\lambda}(u)\overline{g_{\lambda}(v)} q^{-1} \sum_{0 \leq h < q} e\left(\frac{h}{q}(v + r - u)\right)\]

\[= \frac{1}{q} \sum_{0 \leq u, v < q} [v + r \equiv u \mod q] g_{\lambda}(u)\overline{g_{\lambda}(v)}\]

\[= \frac{1}{q} \sum_{w_1 \leq u, v < w_{i+1}} [v + r \equiv u \mod q] g_{\lambda}(u)\overline{g_{\lambda}(v)}\]

\[= \frac{1}{q} \sum_{w_1 \leq u < w_{i+1} - r} g_{\lambda}(v + r)\overline{g_{\lambda}(v)} + O\left(\frac{r}{q}\right).\]

Lemma 2.8. Let \( H \geq 1 \) be an integer and \( R \) a real number. For all real numbers \( t \) we have

\[
\sum_{h < H} \left| \frac{1}{R} \sum_{r < R} e\left(r(t + h/H)\right) \right|^2 \leq \frac{H + R - 1}{R}.
\]

This lemma is an immediate consequence of the analytic form of the large sieve, see [13, Theorem 3]. This form of the theorem, featuring the optimal constant \( N - 1 + \delta^{-1} \), is due to Selberg.

Lemma 2.9 (Selberg). Let \( N \geq 1, R \geq 1, M \) be integers, \( \alpha_1, \ldots, \alpha_R \in \mathbb{R} \) and \( a_{M+1}, \ldots, a_{M+N} \in \mathbb{C} \). Assume that \( \|\alpha_r - \alpha_s\| \geq \delta \) for \( r \neq s \). Then

\[
\sum_{r=1}^{R} \left| \sum_{n=M+1}^{M+N} a_n e(n\alpha_r) \right|^2 \leq \left( N - 1 + \delta^{-1} \right) \sum_{n=M+1}^{M+N} |a_n|^2.
\]

As an important first step in the proof of Theorem 1.1, we show that for the functions in question we have the following uniformity property.

Proposition 2.10. Let \( g \) be a bounded \( \alpha \)-multiplicative function. Assume that the Fourier–Bohr spectrum of \( g \) is empty, that is,

\[
\left| \sum_{0 \leq n < N} g(n) e(-n\beta) \right| = o(N)
\]

as \( N \to \infty \) for all \( \beta \in \mathbb{R} \). Then

\[
\sup_{\beta \in \mathbb{R}} \left| \sum_{0 \leq n < N} g(n) e(-n\beta) \right| = o(N).
\]
Proof of Proposition 2.10. Without loss of generality we may assume that $|g| \leq 1$, since the full statement follows by scaling. We first prove the special case

$$
\lim_{i \to \infty} \sup_{\beta \in \mathbb{R}} \frac{1}{q_i} \left| \sum_{0 \leq n < q_i} g(n) e(-n\beta) \right| = 0.
$$

We set $h(n) = g(n) e(-n\beta)$ and

$$
S_i = S_i(\beta) = \frac{1}{q_i} \sum_{0 \leq n < q_i} h(n).
$$

For all $i \geq 1$ we have

$$
S_{i+1} = \frac{1}{q_{i+1}} \sum_{0 \leq b < a_{i+1}} \sum_{0 \leq u < q_i} h(u + bq_i) + \frac{1}{q_{i+1}} \sum_{0 \leq u < q_{i-1}} h(u + a_{i+1}q_i) = \frac{q_i}{q_{i+1}} \left( \sum_{0 \leq b < a_{i+1}} h(bq_i) \right) \cdot S_i + \frac{q_i - 1}{q_{i+1}} h(a_{i+1}q_i) S_{i-1}.
$$

Using the recurrence for $q_i$, it follows that $|S_{i+1}| \leq \max\{|S_i|, |S_{i-1}|\}$. By Lemma 2.4 we obtain the statement.

We proceed to the general case. We consider partial sums of $g(n) e(n\beta)$ up to $N$. Assume that $w_i \leq N < w_{i+1}$. We have

$$
\left| \sum_{0 \leq n < N} g(n) e(n\beta) \right|^2 \leq \sum_{0 \leq n < w_i} g(n) e(n\beta) \left( \sum_{0 \leq n, n+r < w_i} g(n+r) \left| g(n) \right| \right) + q_\lambda^2 + 2Nq_\lambda.
$$

We apply the inequality of van der Corput (Lemma 2.1) to obtain

$$
\left| \sum_{0 \leq n < w_i} g(n) e(n\beta) \right|^2 \leq \frac{N + R - 1}{R} \sum_{|r| < R} \left( 1 - \left| \frac{r}{R} \right| \right) e(r\beta) \sum_{0 \leq n, n+r < w_i} g(n+r) \left| g(n) \right|.
$$

We adjust the summation range by omitting the condition $0 \leq n + r < w_i$. This introduces an error term $O(NR)$. Moreover, $\alpha$-multiplicative functions satisfy Lemma 2.6, therefore we may replace $g$ by $g_\lambda$ for the price of another error term, $O(N^2 Rq_\lambda^{-1})$. Using (2.2) we get

$$
\left| \sum_{0 \leq n < w_i} g(n) e(n\beta) \right|^2 \ll \frac{N}{R} \sum_{|r| < R} \left( 1 - \left| \frac{r}{R} \right| \right) e(r\beta) \left( \sum_{0 \leq n < w_i} g_\lambda(n+r) g_\lambda(n) \right) + O\left( R + \frac{NR}{q_\lambda - 1} \right)
$$

$$
\ll NR + \frac{N^2 R}{q_\lambda - 1} + \frac{N}{R} w_i \sum_{h < q_\lambda} \left| G_\lambda(h) \right|^2 \sum_{|r| < R} \left( 1 - \left| \frac{r}{R} \right| \right) e\left( r\beta + \frac{h}{q_\lambda} \right).
$$
Note that the sum over \( r \) is a nonnegative real number. This follows from the identity
\[
\sum_{|r| < R} (R - |r|) e(rx) = \left| \sum_{0 \leq r < R} e(rx) \right|^2,
\]
which can be proved by an elementary combinatorial argument. We use this equation and collect the error terms to get
\[
\left| \frac{1}{N} \sum_{0 \leq n < N} g(n) e(n\beta) \right|^2 \ll \frac{q_\lambda^2}{N^2} + \frac{q_\lambda}{N} + \frac{R}{N \lambda} + \frac{R}{\lambda - 1},
\]
\[
+ \sum_{0 \leq h < q_\lambda} \left| G_\lambda(h) \right|^2 \left| \frac{1}{R} \sum_{0 \leq r < R} e \left( r \left( \beta + \frac{h}{q_\lambda} \right) \right) \right|^2.
\]
Next, using Lemma 2.8 we get
\[
\sum_{0 \leq h < q_\lambda} \left| G_\lambda(h) \right|^2 \left| \frac{1}{R} \sum_{0 \leq r < R} e \left( r \left( \beta + \frac{h}{q_\lambda} \right) \right) \right|^2 \leq \sup_{0 \leq h < q_\lambda} \left| G_\lambda(h) \right|^2 \frac{q_\lambda + R - 1}{R}.
\]

In order to establish the existence of the correlation \( \gamma_r \) of \( g \) for all \( r \geq 0 \), we use the following theorem [10, Théorème 4]. (Note that we defined \( \psi_\lambda(n) = \sum_{0 \leq i < \lambda} \varepsilon_i(n)q_i \).)

**Lemma 2.11** (Coquet–Rhin–Toffin). Let \( \lambda \geq 1 \) and \( a < q_\lambda \). The set \( \mathcal{E}(\lambda, a) = \{ n \in \mathbb{N} : \psi_\lambda(n) = a \} \) possesses an asymptotic density given by
\[
\delta = (q_\lambda + q_{\lambda - 1}[0; a_{\lambda+1}, \ldots])^{-1} \quad \text{if } a \geq q_{\lambda-1};
\]
\[
\delta' = (1 + [0; a_{\lambda+1}, \ldots])^{-1} \quad \text{if } a < q_{\lambda-1}.
\]

**Lemma 2.12.** Let \( g \) be a bounded \( \alpha \)-multiplicative function. Then for every \( r \geq 0 \) the limit
\[
\lim_{N \to \infty} \frac{1}{N} \sum_{n < N} g(n + r)\bar{g}(n)
\]
exists.

We note that the existence of the correlation was established in [10] for the special case that \( g(n) = e(y\sigma_\alpha(n)) \), where \( e(x) = e^{2\pi ix} \) and \( y \in \mathbb{R} \).
Proof. Let \( \lambda, N \geq 0 \) and \( r \geq 1 \) and set \( k = \max \{ j : w_j \leq N \} \). Moreover, let \( a = a(N) \) be the number of indices \( j < k \) such that \( w_{j+1} - w_j = q_\lambda \) and \( b = b(N) \) be the number of indices \( j < k \) such that \( w_{j+1} - w_j = q_{\lambda-1} \). By Lemma 2.11 \( a(N)/N \) and \( b(N)/N \) converge, say to \( A \) and \( B \) respectively. Let \( \lambda \) be so large that \( r/q\lambda - 1 < \varepsilon \). Moreover, choose \( N_0 \) so large that

\[
\left| A - a(N)/N \right| < \varepsilon q_{\lambda-1}, \quad \left| B - b(N)/N \right| < \varepsilon q_{\lambda-1} \text{ and } q\lambda/N < \varepsilon \text{ for all } N \geq N_0.
\]

Then by Lemma 2.6 we get

\[
\sum_{0 \leq n < N} g(n + r)\overline{g(n)} = \sum_{0 \leq n < N} g_\lambda(n + r)\overline{g_\lambda(n)} + O(Nrq_{\lambda-1}^{-1})
\]

therefore

\[
\left| \frac{1}{N} \sum_{0 \leq n < N} g(n + r)\overline{g(n)} - A \sum_{0 \leq n < q_\lambda} g_\lambda(n + r)\overline{g_\lambda(n)} - B \sum_{0 \leq n < q_{\lambda-1}} g_\lambda(n + r)\overline{g_\lambda(n)} \right|
\]

\[
\ll \left| \frac{1}{N} \sum_{0 \leq n < N} g(n + r)\overline{g(n)} - \frac{a}{N} \sum_{0 \leq n < q_\lambda} g_\lambda(n + r)\overline{g_\lambda(n)} \right| + 2\varepsilon
\]

\[
= \left| \frac{1}{N} \sum_{0 \leq n < N} g(n + r)\overline{g(n)} - \frac{1}{N} \sum_{0 \leq n < w_k} g_\lambda(n + r)\overline{g_\lambda(n)} \right| + 2\varepsilon
\]

\[
\ll \frac{q_\lambda}{N} + \frac{r}{q_{\lambda-1}} + 2\varepsilon.
\]

By the triangle inequality it follows that the values \( \frac{1}{N} \sum_{n < N} g(n + r)\overline{g(n)} \) form a Cauchy sequence and therefore a convergent sequence, which proves the existence of the correlation of \( g \).

\[
\square
\]

3. Proof of the theorem

Now we are prepared to prove Theorem 1.1. If \( g \) is pseudorandom, then by Lemma 2.3 its spectrum is empty. We are therefore concerned with the converse. Let \( \ell \geq 0 \). We denote by \( a \) the number of \( i < \ell \) such that \( w_{i+1} - w_i = q_\lambda \) and by \( b \) the number of \( i < \ell \) such that \( w_{i+1} - w_i = q_{\lambda-1} \).

Choose \( \varepsilon_r \) such that \( |\varepsilon_r| = 1 \) and

\[
\varepsilon_r \sum_{0 \leq h < q_\lambda} |G_\lambda(h)|^2 e(hrq_{\lambda-1}^{-1})
\]
is a nonnegative real number. Similarly choose $\varepsilon'_r$ for $\lambda - 1$. We have

$$
\frac{1}{R} \sum_{0 \leq r < R} \left| \frac{1}{w_\ell} \sum_{0 \leq n < w_\ell} g_\lambda(n + r)g_\lambda(n) \right|
$$

$$
= \frac{a q_\lambda}{w_\ell} \frac{1}{R} \sum_{0 \leq r < R} \varepsilon_r \sum_{0 \leq h < q_\lambda} |G_\lambda(h)|^2 e\left(\frac{hr}{q_\lambda}\right)
$$

$$
+ \frac{b q_\lambda - 1}{w_\ell} \frac{1}{R} \sum_{0 \leq r < R} \varepsilon'_r \sum_{0 \leq h < q_\lambda - 1} |G_{\lambda - 1}(h)|^2 e\left(\frac{hr}{q_{\lambda - 1}}\right) + O\left(\frac{ar}{w_\ell} + \frac{br}{w_\ell}\right)
$$

$$
= \frac{1}{R} \left| \frac{a q_\lambda}{w_\ell} \sum_{0 \leq h < q_\lambda} |G_\lambda(h)|^2 \sum_{0 \leq r < R} \varepsilon_r e\left(\frac{hr}{q_\lambda}\right) \right|
$$

$$
+ \frac{b q_\lambda - 1}{w_\ell} \sum_{0 \leq h < q_\lambda - 1} |G_{\lambda - 1}(h)|^2 \sum_{0 \leq r < R} \varepsilon'_r e\left(\frac{hr}{q_{\lambda - 1}}\right) + O\left(\frac{r}{q_{\lambda - 1}}\right).
$$

By Cauchy-Schwarz we obtain

$$
\frac{1}{R^2} \left| \sum_{0 \leq h < q_\lambda} |G_\lambda(h)|^2 \sum_{0 \leq r < R} \varepsilon_r e\left(\frac{hr}{q_\lambda}\right) \right|^2
$$

$$
\leq \frac{1}{R^2} \sum_{0 \leq h < q_\lambda} |G_\lambda(h)|^4 \sum_{0 \leq r < R} \varepsilon_r e\left(\frac{hr}{q_\lambda}\right)^2
$$

$$
\leq \frac{1}{R^2} \sum_{0 \leq h < q_\lambda} |G_\lambda(h)|^4 \sum_{0 \leq r_1, r_2 < R} \varepsilon_{r_1} \varepsilon_{r_2} e\left(h - \frac{r_1 - r_2}{q_\lambda}\right)
$$

$$
= \frac{q_\lambda}{R^2} \sum_{0 \leq h < q_\lambda} |G_\lambda(h)|^4 \sum_{0 \leq r_1, r_2 < R} \varepsilon_{r_1} \varepsilon_{r_2} \delta_{r_1, r_2}
$$

$$
= \frac{q_\lambda}{R} \sum_{0 \leq h < q_\lambda} |G_\lambda(h)|^4,
$$
Similarly for $\lambda - 1$. Using Lemma 2.6, we get
\[
\frac{1}{R} \sum_{0 \leq r < R} |\gamma_r| = \lim_{k \to \infty} \frac{1}{R} \sum_{0 \leq r < R} \frac{1}{w_{\ell}} \sum_{0 \leq n < w_{\ell}} g(n + r)\overline{g(n)}
\]
\[
= \lim_{k \to \infty} \frac{1}{R} \sum_{0 \leq r < R} \frac{1}{w_{\ell}} \sum_{0 \leq n < w_{\ell}} g_\lambda(n + r)\overline{g_\lambda(n)} + O\left(\frac{R}{q_{\lambda - 1}}\right)
\]
\[
\leq \left[ \left( \sum_{0 \leq h < q_{\lambda - 1}} |G_{\lambda - 1}(h)|^4 \right)^{1/2} + \left( \sum_{0 \leq h < q_{\lambda}} |G_\lambda(h)|^4 \right)^{1/2} \right] \left( \frac{q_{\lambda}}{R} \right)^{1/2} + O\left(\frac{R}{q_{\lambda - 1}}\right)
\]
Using the hypothesis and Proposition 2.10, we get $\sup_{h \in \mathbb{Z}} |G_\lambda(h)| = o(1)$ as $\lambda \to \infty$. By Parseval’s identity this implies
\[
\sum_{h < q_{\lambda}} |G_\lambda(h)|^4 = o(1).
\]
By a straightforward argument we conclude that
\[
\frac{1}{R} \sum_{0 \leq r < R} |\gamma_r| = o(1)
\]
as $R \to \infty$. Since $g$ is bounded, an application of Lemma 2.2 completes the proof of Theorem 1.1.

References


Lukas Spiegelhofer
Institute of Discrete Mathematics and Geometry,
Vienna University of Technology
Wiedner Hauptstrasse 8–10
1040 Vienna, Austria
E-mail: lukas.spiegelhofer@tuwien.ac.at
URL: http://dmg.tuwien.ac.at/spiegelhofer/