FUNCTIONAL LIMIT THEOREMS FOR DIGITAL EXPANSIONS

MICHAEL DRMOTA, MICHAEL FUCHS, AND EUGENIJUS MANSTAVIČIUS

ABSTRACT. The main purpose of this paper is to discuss the asymptotic behavior of the difference $s_{q,k}(P(n)) - k(q-1)/2$ where $s_{q,k}(n)$ denotes the sum of the first k digits in the q-ary digital expansion of n and $P(x)$ is an integer polynomial. We prove that this difference can be approximated by a Brownian motion and obtain under special assumptions on P a Strassen's type version of the law of the iterated logarithm. Furthermore, we extend these results to the joint distribution of q_1-ary and q_2-ary digital expansions where q_1 and q_2 are coprime.

1. INTRODUCTION

Let $q > 1$ be a given integer. A real-valued function f defined on the non-negative integers is said to be q-additive if $f(0) = 0$ and

$$f(n) = \sum_{j\ge 0} f(a_{q,j}(n)q^j) \quad \text{for} \quad n = \sum_{j\ge 0} a_{q,j}(n)q^j$$

where $a_{q,j}(n) \in E_q := \{0, 1, \ldots, q-1\}$. A special q-additive function is the sum-of-digits function

$$s_q(n) = \sum_{j\ge 0} a_{q,j}(n).$$

In order to keep notation as simple as possible on the one hand and to make the ideas of the proofs as lucid as possible on the other hand, we are mainly interested in the sum-of-digits function although all results of the paper can immediately be extended to more general q-additive functions. In a final section, we are going to outline the more general case.

The statistical behavior of the sum-of-digits function and more generally for q-additive function has been very well studied by several authors (compare with the references stated in [6]).

It is also very interesting to consider the partial sum-of-digits function

$$s_{q,k}(n) := \sum_{0\le j\le k} a_{q,j}(n).$$

The sequence $(s_{q,k}(n))_{k\ge 0}$ may be considered as an increasing *random walk* and really encodes the digital expansion of n.

Here and in what follows, we assume that every integer $n \in \{0, 1, 2, \ldots, N-1\}$ is equally likely [1] i.e. we consider the probability space $(\mathbb{N}_0, \mathcal{P}(\mathbb{N}_0), \nu_N)$ where $\mathcal{P}(\mathbb{N}_0)$

1991 *Mathematics Subject Classification.* Primary: 11A63, Secondary: 11N60.

Key words and phrases. q-ary digital expansion, sum-of-digits function, functional limit theorem, Strassen's law of the iterated logarithm.

The first two authors were supported by the Austrian Science Foundation FWF, grant S8302-MAT.

[1] We will also consider the first $\pi(N)$ primes $p \le N$ and assume that they are equally likely.

denotes the powerset of $\mathbb{N}_0$ and ν_N is the probability measure defined by

$$\nu_N(A) := \frac{1}{N}\#\{0 \leq n < N | n \in A\} \quad A \in \mathcal{P}(\mathbb{N}_0).$$

On this probability space, we introduce the following stochastic process

$$X_N(t)(n) := \left(\frac{1}{\sigma_q\sqrt{L}}\left(s_{q,tL}(n) - tL\frac{q-1}{2}\right)\right)$$

for $t = i/L, i = 0, \ldots, [L]$ and by linearizing otherwise where $L := L_q := \log_q N$ and $\sigma_q := \sqrt{(q^2-1)/12}$.

Throughout the paper, we are mainly interested in stochastic processes with continues paths. If in the following the path is only defined on a finite number of points in $[0,1]$ then, we always use linear interpolation in order to get a continues function.

In [13] the third author has proved the following functional limit theorem:

Theorem 1. *We have, as $N \to \infty$,*

$$X_N(t) \to B(t)$$

where $B(t)$ denotes the standard Brownian motion and weak convergence is considered in the space $C[0,1]$.

As an immediate corollary, we have:

Corollary 1. *We have, as $N \to \infty$,*

$$\max_{0\leq t\leq 1} |X_N(t)| \to \max_{0\leq t\leq 1} |B(t)|.$$

Furthermore in [14], the third author continued his investigations started in [13] and obtained for the partial sum-of-digits function a law of the iterated logarithm. In order to state the result, we need few more notation.

For processes $Y_{N,k}$, $k \leq m_N \in \mathbb{N}_0$ defined on some probability space $(\Omega_N, \mathcal{F}_N, P_N)$, we use the notation

$$Y_{N,k} \Longrightarrow \mathcal{K} \quad (P_N - a.s.)$$

if the following two relations hold:

$$\lim_{x\longrightarrow\infty} \limsup_{N\longrightarrow\infty} P_N\left(\max_{x\leq k\leq m_N} \rho(Y_{N,k}, \mathcal{K}) \geq \epsilon\right) = 0$$

and

$$\lim_{x\longrightarrow\infty} \liminf_{N\longrightarrow\infty} P_N\left(\min_{x\leq k\leq m_N} \rho(Y_{N,k}, X) < \epsilon\right) = 1$$

for arbitrary $\epsilon > 0$ and $X \in \mathcal{K}$. Here, as usually ρ is the maximum norm, $\rho(X, \mathcal{A}) = \inf\{\rho(X,Y) | Y \in \mathcal{A}\}$, and $\mathcal{K}$ denotes the Strassen's set.

We define stochastic processes on $(\mathbb{N}_0, \mathcal{P}(\mathbb{N}_0), \nu_N)$ by

$$S_{N,k}(t)(n) = \frac{1}{\sigma_q\sqrt{2k\log\log k}}\left(s_{q,tk}(n) - tk\frac{q-1}{2}\right)$$

where $t = i/k, i = 0, \ldots, k$ and $k \leq L$. Then the third author has proved in [14]:

Theorem 2. *We have*

$$S_{N,k} \Longrightarrow \mathcal{K} \quad (\nu_N - a.s.).$$

The purpose of this paper is to generalize these properties to the partial sum-of-digits function on polynomial sequences and it is organized as follows: in Section 2 the results are stated, Section 3 is devoted to the proofs of the functional limit theorems and these results are sharpened in Section 4 by showing convergence of all moments. In Section 5, we are concerned with the functional version of the iterated logarithm law and in a final section, we outline possible extensions of the results.

2. Results

Our first result is a direct generalization of Theorem 1 to polynomial sequences on integers and on primes.

Therefore let $P(x)$ be a polynomial with integer coefficients, degree r, and positive leading term and define stochastic processes by

$$X_{N,P,q}(t)(n) := X_{N,P}(t)(n) := \frac{1}{\sigma_q\sqrt{rL}}\left(s_{q,trL}(P(n)) - trL\frac{q-1}{2}\right)$$

and

$$Y_{N,P,q}(t)(p) := Y_{N,P}(t)(p) := \frac{1}{\sigma_q\sqrt{rL}}\left(s_{q,trL}(P(p)) - trL\frac{q-1}{2}\right)$$

where $t = i/rL, i = 0, \ldots, [rL]$. The only difference between $X_{N,P}$ and $Y_{N,P}$ is, that the second process is defined on primes. With this notation, we have:

Theorem 3. *Let $q \geq 2$ and $P(x)$ be an integer polynomial of degree $r \geq 1$ with positive leading term. Then, we have, as $N \to \infty$,*

$$X_{N,P}(t) \to B(t)$$

and

$$Y_{N,P}(t) \to B(t).$$

As above, we get as an corollary:

Corollary 2. *We have, as $N \to \infty$,*

$$\max_{0\leq t\leq 1} |X_{N,P}(t)| \to \max_{0\leq t\leq 1} |B(t)|$$

and

$$\max_{0\leq t\leq 1} |Y_{N,P}(t)| \to \max_{0\leq t\leq 1} |B(t)|.$$

It is also possible to sharpen Corollary 2 to convergence of moments.

Theorem 4. *Let $q \geq 2$ and $P(x)$ be an integer polynomial of degree $r \geq 1$ with positive leading term. Then, for every integer $k \geq 1$, we have, as $N \to \infty$,*

$$\mathbf{E}\left(\max_{0\leq t\leq 1} |X_{N,P}(t)|\right)^k \to \mathbf{E}\left(\max_{0\leq t\leq 1} |B(t)|\right)^k$$

and

$$\mathbf{E}\left(\max_{0\leq t\leq 1} |Y_{N,P}(t)|\right)^k \to \mathbf{E}\left(\max_{0\leq t\leq 1} |B(t)|\right)^k.$$

This result is even of some interest if we consider just $P(x) = x$ and $k = 1$. We have, as $N \to \infty$,

$$\frac{1}{N} \sum_{n<N} \max_{0 \le k \le \log_q N} \left| s_{q,k}(n) - k\frac{q-1}{2} \right| \sim \sqrt{\frac{2}{\pi}} \cdot \sqrt{\frac{q^2-1}{12} \log_q N}.$$

The above properties even generalize to the joint distribution of two different digital expansions.

Theorem 5. *Let $q_1, q_2 \ge 2$ be coprime and $P_1(x), P_2(x)$ be two integer polynomials of degrees $r_1, r_2 \ge 1$ with positive leading term. Then, we have, as $N \to \infty$,*

$$(X_{N,P_1,q_1}(t_1), X_{N,P_1,q_2}(t_2)) \to (B_1(t_1), B_2(t_2))$$

and

$$(Y_{N,P_1,q_1}(t_1), Y_{N,P_1,q_2}(t_2)) \to (B_1(t_1), B_2(t_2))$$

where $(B_1(t_1), B_2(t_2))$ denotes a Gaussian field consisting of two independent Brownian motions.

Corollary 3. *We have, as $N \to \infty$,*

$$\left(\max_{0 \le t_1 \le 1} |X_{N,P_1,q_1}(t_1)|, \max_{0 \le t_2 \le 1} |X_{N,P_2,q_2}(t_2)| \right) \to \left(\max_{0 \le t_1 \le 1} |B_1(t_1)|, \max_{0 \le t_2 \le 1} |B_2(t_2)| \right)$$

and

$$\left(\max_{0 \le t_1 \le 1} |Y_{N,P_1,q_1}(t_1)|, \max_{0 \le t_2 \le 1} |Y_{N,P_2,q_2}(t_2)| \right) \to \left(\max_{0 \le t_1 \le 1} |B_1(t_1)|, \max_{0 \le t_2 \le 1} |B_2(t_2)| \right).$$

As above it is possible to sharpen this corollary.

Theorem 6. *Let $q_1, q_2 \ge 2$ be coprime and $P_1(x), P_2(x)$ be two integer polynomials of degrees $r_1, r_2 \ge 1$ with positive leading term. Then for all integers $k_1, k_2 \ge 0$, we have, as $N \to \infty$,*

$$\mathbf{E} \left(\max_{0 \le t_1 \le 1} |X_{N,P_1,q_1}(t_1)| \right)^{k_1} \left(\max_{0 \le t_2 \le 1} |X_{N,P_2,q_2}(t_2)| \right)^{k_2} \to \mathbf{E} \left(\max_{0 \le t_1 \le 1} |B(t_1)| \right)^{k_1} \left(\max_{0 \le t_2 \le 1} |B(t_2)| \right)^{k_2}$$

and

$$\mathbf{E} \left(\max_{0 \le t_1 \le 1} |Y_{N,P_1,q_1}(t_1)| \right)^{k_1} \left(\max_{0 \le t_2 \le 1} |Y_{N,P_2,q_2}(t_2)| \right)^{k_2} \to \mathbf{E} \left(\max_{0 \le t_1 \le 1} |B(t_1)| \right)^{k_1} \left(\max_{0 \le t_2 \le 1} |B(t_2)| \right)^{k_2}.$$

Theorem 5 may be considered as a theoretical justification to the statement that two q-ary digital expansions with coprime q are (asymptotically) independent.

Now, let us turn to the law of the iterated logarithm. Therefore, we define for a polynomial $P(x)$ with integer coefficients, degree r, and positive leading term, the following processes

$$S_{N,k,P,q}(t)(n) := S_{N,k,P}(t)(n) := \frac{1}{\sigma_q \sqrt{2k \log\log k}} \left(s_{q,tk}(P(n)) - tk\frac{q-1}{2} \right)$$

where $t = i/k, i = 0, \ldots, k$ and $k \le rL$.

One might expect that these processes obey a law of the iterated logarithm of the form given in Theorem 2. Although, we were not able to prove this in general, we can state the following partial result towards a more general result:

Theorem 7. *Let $q \geq 2$ and $P(x)$ be a polynomial with integer coefficients of degree $r \geq 1$ and positive leading term which is a permutation polynomial for every power of q. Consider the processes $S_{N,k,P}$ introduced above for $k \leq L$. Then, we have*

$$S_{N,k,P} \Longrightarrow \mathcal{K} \quad (\nu_N - a.s.).$$

We have the following easy consequence:

Corollary 4. *With assumptions as in Theorem 7, we have*

$$S_{N,k,P}(1) \Longrightarrow [-1,1] \quad (\nu_N - a.s.).$$

This result can also be extended to the joint distribution of q_1-ary and q_2-ary digital expansions.

We use the notation $\mathcal{K}_1 = \mathcal{K} \times \mathcal{K}$ for the two-dimensional Strassen's set and $\mathcal{K}_2$ for the set of all pairs (f_1, f_2), where $f_i, i = 1,2$ are absolutely continuous functions on $[0,1]$ with $f_i(0) = 0, i = 1,2$ and

$$\int_0^1 (f_1'(t)^2 + f_2'(t)^2)dt \leq 1.$$

For two-dimensional processes $(Y_{N,k_1}, Z_{N,k_2}), (k_1,k_2) \in M_N \subseteq \mathbb{N}_0^2$ defined on some probability spaces $(\Omega_N, \mathcal{F}_N, P_N)$, we use the notation

$$(Y_{N,k_1}, Z_{N,k_2}) \Longrightarrow \bar{\mathcal{K}} \quad (P_N - a.s.)$$

(where $\bar{\mathcal{K}}$ is either $\mathcal{K}_1$ or $\mathcal{K}_2$) if the following two relations hold:

$$\lim_{x \longrightarrow \infty} \limsup_{N \longrightarrow \infty} P_N \left(\max_{k_1,k_2 \geq x, (k_1,k_2) \in M_N} \rho((Y_{N,k_1}, Z_{N,k_2}), \bar{\mathcal{K}}) \geq \epsilon \right) = 0$$

and

$$\lim_{x \longrightarrow \infty} \liminf_{N \longrightarrow \infty} P_N \left(\min_{k_1,k_2 \geq x, (k_1,k_2) \in M_N} \rho((Y_{N,k_1}, Z_{N,k_2}), (X_1, X_2)) < \epsilon \right) = 1$$

for arbitrary $\epsilon > 0$ and $(X_1, X_2) \in \bar{\mathcal{K}}$. Here, ρ denotes again the maximum norm.

With this notation, we have the following result for the joint distribution of q_1-ary and q_2-ary digital expansions:

Theorem 8. *Let $q_1, q_2 \geq 2$ and $P_i(x), i = 1,2$ be two polynomials with integer coefficients, degrees $r_i \geq 1, i = 1,2$, and positive leading terms. Furthermore, we assume that $P_i(x)$ is a permutation polynomial for all powers of q_i, $i = 1,2$.*

(1) *The processes $(S_{N,k_1,P_1,q_1}, S_{N,k_2,P_2,q_2})$ with $k_1 \leq L_{q_1}$ and $k_2 \leq L_{q_2}$ satisfy*
$$(S_{N,k_1,P_1,q_1}, S_{N,k_2,P_2,q_2}) \Longrightarrow \mathcal{K}_1 \quad (\nu_N - a.s.).$$
(2) *Let $(q_1, q_2) = 1$. Then the processes $(S_{N,k,P_1,q_1}, S_{N,k,P_2,q_2})$ with $k \leq L_{q_1 q_2}$ satisfy*
$$(S_{N,k,P_1,q_1}, S_{N,k,P_2,q_2}) \Longrightarrow \mathcal{K}_2 \quad (\nu_N - a.s.).$$

Again, we have the following simple consequence:

Corollary 5. *Suppose that the assumptions of Theorem 8 are satisfied. Then, we have:*

(1) *The processes* $(S_{N,k_1,P_1,q_1}, S_{N,k_2,P_2,q_2})$ *with* $k_1 \le L_{q_1}$ *and* $k_2 \le L_{q_2}$ *satisfy*

$$(S_{N,k_1,P_1,q_1}(1), S_{N,k_2,P_2,q_2}(1)) \Longrightarrow [-1,1]^2 \quad (\nu_N - a.s.).$$

(2) *Let* $(q_1,q_2)=1$. *Then the processes* $(S_{N,k,P_1,q_1}, S_{N,k,P_2,q_2})$ *with* $k \le L_{q_1q_2}$ *satisfy*

$$(S_{N,k,P_1,q_1}(1), S_{N,k,P_2,q_2}(1)) \Longrightarrow \{(x,y)|x^2+y^2\le 1\} \quad (\nu_N - a.s.).$$

3. Comparison of Moments

Let $q>1$ be an integer and $P(x)$ a polynomial with integer coefficients, degree r, and a positive leading term. We consider the stochastic processes $X_{N,P}(t)$ and $Y_{N,P}(t)$ introduced in section 2 together with the truncated versions

$$\tilde{X}_{N,P}(t)(n) := \frac{1}{\sigma_q\sqrt{rL}}\left(\sum_{I\le j\le J(t)}\left(a_{q,j}(P(n)) - \frac{q-1}{2}\right)\right)$$

and

$$\tilde{Y}_{N,P}(t)(p) := \frac{1}{\sigma_q\sqrt{rL}}\left(\sum_{I\le j\le J(t)}\left(a_{q,j}(P(p)) - \frac{q-1}{2}\right)\right)$$

where $I=\lceil(\log N)^\eta\rceil$, $J(t)=\min\{\lfloor trL\rfloor, \lfloor rL-(\log N)^\eta\rfloor\}$, $t=i/rL, i=0,\dots,[rL]$, and $0<\eta<1/2$ is an arbitrary real number. Since

$$\sup_{0\le t\le 1}|X_{N,P}(t)(n) - \tilde{X}_{N,P}(t)(n)| \ll L^{\eta-\frac{1}{2}}$$

and

$$\sup_{0\le t\le 1}|Y_{N,P}(t)(p) - \tilde{Y}_{N,P}(t)(p)| \ll L^{\eta-\frac{1}{2}},$$

we have, as $N\longrightarrow\infty$,

$$X_{N,P}(t)-\tilde{X}_{N,P}(t)\to 0$$

and

$$Y_{N,P}(t)-\tilde{Y}_{N,P}(t)\to 0.$$

Hence, it is enough to prove Theorem 2 for the truncated processes.

The following Lemma is contained in [1].

Lemma 1. *Let* $\lambda>0$ *be a real constant,* $k_1,\dots,k_h$ *integers with*

$$(\log N)^\eta \le k_1 < k_2 < \cdots < k_h \le rL-(\log N)^\eta$$

and $b_j\in E_q, 1\le j\le h$. *Then, we uniformly have, as* $N\longrightarrow\infty$,

$$\frac{1}{N}\#\{n<N|a_{q,k_j}(P(n))=b_j, 1\le j\le h\} = \frac{1}{q^h}+\mathcal{O}\left(L^{-\lambda}\right)$$

and

$$\frac{1}{\pi(N)}\#\{p\le N|a_{q,k_j}(P(p))=b_j, 1\le j\le h\} = \frac{1}{q^h}+\mathcal{O}\left(L^{-\lambda}\right).$$

We use this Lemma to prove the following Proposition.

Proposition 1. *Let $0 \le t_1 < \ldots < t_h \le 1$ be real numbers. Then for all integers $l_1, \ldots, l_h \ge 1$, we have, as $N \longrightarrow \infty$,*

$$\mathbf{E}\tilde{X}_{N,P}(t_1)^{l_1} \cdots \tilde{X}_{N,P}(t_h)^{l_h} \longrightarrow \mathbf{E}B(t_1)^{l_1} \cdots B(t_h)^{l_h}$$

and

$$\mathbf{E}\tilde{Y}_{N,P}(t_1)^{l_1} \cdots \tilde{Y}_{N,P}(t_h)^{l_h} \longrightarrow \mathbf{E}B(t_1)^{l_1} \cdots B(t_h)^{l_h}.$$

Proof. First of all, we observe that it is enough to show convergence of the mixed moments

$$\mathbf{E}\tilde{X}_{N,P}(t_1)^{l_1}(\tilde{X}_{N,P}(t_2) - \tilde{X}_{N,P}(t_1))^{l_2} \cdots (\tilde{X}_{N,P}(t_h) - \tilde{X}_{N,P}(t_{h-1}))^{l_h}.$$

In order to demonstrate the ideas of the proof, we concentrate ourself on the special case $h = 2$ and $l_1 = l_2 = 2$. The general result follows in the same manner.

We introduce the following stochastic process

$$\bar{X}_{N,P}(t_i)(n) = \frac{1}{\sigma_q\sqrt{rL}} \sum_{j=I}^{J(t_i)} \sum_{b\in E_q} b\left(\delta(a_{q,j}(P(n)), b) - \frac{1}{q}\right) \tag{3.1}$$

where $\delta(x, y)$ is the Kronecker function. It is clear that we have

$$|\tilde{X}_{N,P}(t_i)(n) - \bar{X}_{N,P}(t_i)(n)| \ll L^{-\frac{1}{2}}$$

where the implied constant does not depend on n and therefore, it suffices to show convergence of mixed moments for the stochastic process $\bar{X}_{N,P}$.

Next, we consider

$$\begin{aligned}
&\mathbf{E}\bar{X}_{N,P}(t_1)^2(\bar{X}_{N,P}(t_2) - \bar{X}_{N,P}(t_1))^2 \\
&\quad= \frac{1}{N}\sum_{n<N} \bar{X}_{N,P}(t_1)(n)^2(\bar{X}_{N,P}(t_2)(n) - \bar{X}_{N,P}(t_1)(n))^2 \\
&\quad= \sum_{j_1=I}^{J(t_1)}\sum_{j_2=I}^{J(t_1)}\sum_{j_3=J(t_1)+1}^{J(t_2)}\sum_{j_4=J(t_1)+1}^{J(t_2)}\sum_{b_1\in E_q}\sum_{b_2\in E_q}\sum_{b_3\in E_q}\sum_{b_4\in E_q} \frac{b_1b_2b_3b_4}{\sigma_q^4(rL)^2} \times \\
&\qquad\qquad \times \frac{1}{N}\sum_{n<N}\left(\delta(a_{q,j_1}(P(n)), b_1) - \frac{1}{q}\right)\left(\delta(a_{q,j_2}(P(n)), b_2) - \frac{1}{q}\right) \\
&\qquad\qquad\qquad \left(\delta(a_{q,j_3}(P(n)), b_3) - \frac{1}{q}\right)\left(\delta(a_{q,j_4}(P(n)), b_4) - \frac{1}{q}\right).
\end{aligned}$$

If we consider only the last sum, extract the product, use Corollary 1, and write everything back then, we get, as $N \longrightarrow \infty$,

$$\mathbf{E}\bar{X}_{N,P}(t_1)^2(\bar{X}_{N,P}(t_2) - \bar{X}_{N,P}(t_1))^2 = \mathbf{E}Z_N(t_1)^2(Z_N(t_2) - Z_N(t_1))^2 + \mathcal{O}\left(L^{-\lambda}\right)$$

where $\lambda > 0$ is an arbitrary real constant and the stochastic process $Z_N(t)$ is defined as follows

$$Z_N(t) := \frac{1}{\sigma_q\sqrt{rL}}\left(\sum_{I\le j\le J(t)}\left(\xi_j - \frac{q-1}{2}\right)\right), \quad t \in [0,1]$$

with an independent, identically distributed sequence of random variables ξ_j defined on some probability space by $P(\xi_j = d) = q^{-1}, d \in E_q$.

In the more general case, we would get

$$\begin{aligned}&\mathbf{E}\bar{X}_{N,P}(t_1)^{l_1}(\bar{X}_{N,P}(t_2)-\bar{X}_{N,P}(t_1))^{l_2}\cdots(\bar{X}_{N,P}(t_h)-\bar{X}_{N,P}(t_{h-1}))^{l_h}=\\&\quad=\mathbf{E}Z_N(t_1)^{l_1}(Z_N(t_2)-Z_N(t_1))^{l_2}\cdots(Z_N(t_h)-Z_N(t_{h-1}))^{l_h}+\mathcal{O}\left(L^{-\lambda}\right).\end{aligned}$$

Because of the independence of ξ_j, we have

$$\begin{aligned}&\mathbf{E}\bar{X}_{N,P}(t_1)^{l_1}(\bar{X}_{N,P}(t_2)-\bar{X}_{N,P}(t_1))^{l_2}\cdots(\bar{X}_{N,P}(t_h)-\bar{X}_{N,P}(t_{h-1}))^{l_h}=\\&\quad=\mathbf{E}Z_N(t_1)^{l_1}\mathbf{E}(Z_N(t_2)-Z_N(t_1))^{l_2}\cdots\mathbf{E}(Z_N(t_h)-Z_N(t_{h-1}))^{l_h}+\mathcal{O}\left(L^{-\lambda}\right).\end{aligned}$$

Now, we apply Donsker's theorem on the stochastic process $Z_N(t)$ and hence, as $N\longrightarrow\infty$,

$$Z_N(t)\to B(t)$$

and especially

$$Z_N(t_i)-Z_N(t_{i-1})\to B(t_i)-B(t_{i-1})\quad 1\le i\le h\quad t_0=0.$$

Moreover, using the inequality,

$$\begin{aligned}\mathbf{E}|Z_N(t_i)-Z_N(t_{i-1})|^k&\ll L^{-k/2}(J(t_i)-J(t_{i-1}))^{k/2-1}\sum_{J(t_{i-1})<j\le J(t_i)}\mathbf{E}\left|\xi_j-\frac{q-1}{2}\right|^k\\&\ll(t_i-t_{i-1})^{k/2}\le 1\end{aligned}$$

where $k\ge 2$, we get

$$\mathbf{E}(Z_N(t_i)-Z_N(t_{i-1}))^{l_i}\to\mathbf{E}(B(t_i)-B(t_{i-1}))^{l_i}$$

which together with the above result shows the first part. The second part is proved similarly. □

This Proposition together with the Frechet-Shohat Theorem implies that, as $N\longrightarrow\infty$,

$$(\tilde{X}_{N,P}(t_1),\ldots,\tilde{X}_{N,P}(t_h))\to(B(t_1),\ldots,B(t_h))$$

and

$$(\tilde{Y}_{N,P}(t_1),\ldots,\tilde{Y}_{N,P}(t_h))\to(B(t_1),\ldots,B(t_h)).$$

The next step is a tightness inequality.

Proposition 2. *For every even integer $l\ge 0$ there exists a positive real constant C such that for all N and all $0\le s,t\le 1$, we have*

$$\mathbf{E}|\tilde{X}_{N,P}(s)-\tilde{X}_{N,P}(t)|^l\le C|s-t|^{l/2}$$

resp.

$$\mathbf{E}|\tilde{Y}_{N,P}(s)-\tilde{Y}_{N,P}(t)|^l\le C|s-t|^{l/2}.$$

Proof. First of all it is an easy exercise to show that it is sufficient to prove the assertion for $0\le s,t\le 1$ with $sL,tL\in\mathbb{Z}$. Furthermore, we can assume w.l.o.g. that $s>t$.

Repeating the first part of the proof of Proposition 1 together with a more careful look on the involved error term implies

$$\mathbf{E}\left(\tilde{X}_{N,P}(s)-\tilde{X}_{N,P}(t)\right)^l=\mathbf{E}(Z_N(s)-Z_N(t))^l+\mathcal{O}\left((s-t)^lL^{-\lambda}\right)$$

where $\lambda>0$ is an arbitrary real number and the stochastic process $Z_N(t)$ is defined as in the proof of Proposition 1.

Next, we apply on

$$\mathbf{E}(Z_N(s) - Z_N(t))^l$$

the same inequality as in the proof of Proposition 1 and hence

$$\mathbf{E}\left(\tilde{X}_{N,P}(s) - \tilde{X}_{N,P}(t)\right)^l \ll (s-t)^{l/2} + (s-t)^l \ll (s-t)^{l/2}$$

which is the claimed result. The proof of the second part is similar. □

The tightness inequality and the remark above together with Prokhorov's Theorem implies the convergence of the process $\tilde{X}_{N,P}$ resp. $\tilde{Y}_{N,P}$ to the Brownian motion. Hence, the untruncated process $X_{N,P}$ resp. $Y_{N,P}$ also converges to the Brownian motion and Theorem 2 is proved.

Let $q_1, q_2 > 1$ be coprime integers and $P_1(x), P_2(x)$ be polynomials with integer coefficients, degrees r_1, r_2, and positive leading terms. We define the following two dimensional processes

$$\mathbf{X}_{N,\mathbf{P},\mathbf{q}}(t_1,t_2) = (X_{N,P_1,q_1}(t_1), X_{N,P_2,q_2}(t_2))$$

and

$$\mathbf{Y}_{N,\mathbf{P},\mathbf{q}}(t_1,t_2) = (Y_{N,P_1,q_1}(t_1), Y_{N,P_2,q_2}(t_2)),$$

and their truncated versions

$$\tilde{\mathbf{X}}_{N,\mathbf{P},\mathbf{q}}(t_1,t_2) = (\tilde{X}_{N,P_1,q_1}(t_1), \tilde{X}_{N,P_2,q_2}(t_2))$$

and

$$\tilde{\mathbf{Y}}_{N,\mathbf{P},\mathbf{q}}(t_1,t_2) = (\tilde{Y}_{N,P_1,q_1}(t_1), \tilde{Y}_{N,P_2,q_2}(t_2))$$

where $\mathbf{P} = (P_1, P_2)$ and $\mathbf{q} = (q_1, q_2)$. It is easy to see that

$$\sup_{0 \le t_1, t_2 \le 1} \|\mathbf{X}_{N,\mathbf{P},\mathbf{q}}(t_1,t_2)(n) - \tilde{\mathbf{X}}_{N,\mathbf{P},\mathbf{q}}(t_1,t_2)(n)\| \ll L^{\eta - \frac{1}{2}}$$

and

$$\sup_{0 \le t_1, t_2 \le 1} \|\mathbf{Y}_{N,\mathbf{P},\mathbf{q}}(t_1,t_2)(p) - \tilde{\mathbf{Y}}_{N,\mathbf{P},\mathbf{q}}(t_1,t_2)(p)\| \ll L^{\eta - \frac{1}{2}}$$

because we know that this is true for each component. Therefore, we have, as $N \longrightarrow \infty$,

$$\mathbf{X}_{N,\mathbf{P},\mathbf{q}}(t_1,t_2) - \tilde{\mathbf{X}}_{N,\mathbf{P},\mathbf{q}}(t_1,t_2) \to 0$$

and

$$\mathbf{Y}_{N,\mathbf{P},\mathbf{q}}(t_1,t_2) - \tilde{\mathbf{Y}}_{N,\mathbf{P},\mathbf{q}}(t_1,t_2) \to 0$$

and it is again enough to consider the truncated processes.

For the proof of Theorem 3, we proceed as in the proof of Theorem 2. First of all, we need a result which is contained in [6] and [8].

Lemma 2. *Let $\lambda > 0$ be a real constant, $k_1^{(i)}, \ldots, k_h^{(i)}, i = 1, 2$ integers with*

$$(\log N)^\eta \le k_j^{(i)} \le r_i \log_{q_i} N - (\log N)^\eta \quad (1 \le j \le h, i = 1, 2)$$

and $b_j^{(i)} \in E_{q_i}, 1 \le j \le h, i = 1, 2$. Then, we uniformly have, as $N \longrightarrow \infty$,

$$\begin{aligned}&\frac{1}{N}\#\{n < N | a_{q_i,k_j^{(i)}}(P_i(n)) = b_j^{(i)}, 1 \le j \le h, i = 1, 2\}\\ &\quad = \prod_{i=1}^{2} \frac{1}{N}\#\{n < N | a_{q_i,k_j^{(i)}}(P_i(n)) = b_j^{(i)}, 1 \le j \le h\} + \mathcal{O}\left(L^{-\lambda}\right)\end{aligned}$$

and

$$\frac{1}{\pi(N)}\#\{p\le N|a_{q_i,k_j^{(i)}}(P_i(p))=b_j^{(i)},1\le j\le h,i=1,2\}$$
$$=\prod_{i=1}^{2}\frac{1}{\pi(N)}\#\{p\le N|a_{q_i,k_j^{(i)}}(P_i(p))=b_j^{(i)},1\le j\le h\}+\mathcal{O}\left(L^{-\lambda}\right).$$

We use this Lemma to prove the following Proposition.

Proposition 3. *Let $0\le t_1^{(i)}<\ldots<t_h^{(i)}\le 1, i=1,2$ be real numbers. Then, for all integer $l_1^{(i)},\ldots,l_h^{(i)}, i=1,2$ and real constants $\lambda>0$, we have, as $N\longrightarrow\infty$,*

$$\mathbf{E}\prod_{i=1}^{2}\tilde{X}_{N,P_i,q_i}(t_1^{(i)})^{l_1^{(i)}}\cdots\tilde{X}_{N,P_i,q_i}(t_h^{(i)})^{l_h^{(i)}}$$
$$=\prod_{i=1}^{2}\mathbf{E}\tilde{X}_{N,P_i,q_i}(t_1^{(i)})^{l_1^{(i)}}\cdots\tilde{X}_{N,P_i,q_i}(t_h^{(i)})^{l_h^{(i)}}+\mathcal{O}\left(L^{-\lambda}\right)$$

and

$$\mathbf{E}\prod_{i=1}^{2}\tilde{Y}_{N,P_i,q_i}(t_1^{(i)})^{l_1^{(i)}}\cdots\tilde{Y}_{N,P_i,q_i}(t_h^{(i)})^{l_h^{(i)}}$$
$$=\prod_{i=1}^{2}\mathbf{E}\tilde{Y}_{N,P_i,q_i}(t_1^{(i)})^{l_1^{(i)}}\cdots\tilde{Y}_{N,P_i,q_i}(t_h^{(i)})^{l_h^{(i)}}+\mathcal{O}\left(L^{-\lambda}\right).$$

Proof. The proof is very similar to the proof of Corollary 2 in [6] and therefore, we omit it. □

This Proposition together with Proposition 1 and the Frechet-Shohat Theorem shows that the first assertion in Prokhorov's Theorem for the process $\tilde{\mathbf{X}}_{N,\mathbf{P},\mathbf{q}}$ resp. $\tilde{\mathbf{Y}}_{N,\mathbf{P},\mathbf{q}}$ is fulfilled. For the second assertion in Prokhorov's Theorem, we need again a tightness inequality (see [16] pp. 473).

Proposition 4. *For every even integer $l\ge 0$ there exists a positive real constant C such that for all N and all $0\le s_1,s_2,t_1,t_2\le 1$, we have*

$$\mathbf{E}\|\tilde{\mathbf{X}}_{N,\mathbf{P},\mathbf{q}}(s_1,s_2)-\tilde{\mathbf{X}}_{N,\mathbf{P},\mathbf{q}}(t_1,t_2)\|^l\le C\|(s_1,s_2)-(t_1,t_2)\|^{l/2}$$

resp.

$$\mathbf{E}\|\tilde{\mathbf{Y}}_{N,\mathbf{P},\mathbf{q}}(s_1,s_2)-\tilde{\mathbf{Y}}_{N,\mathbf{P},\mathbf{q}}(t_1,t_2)\|^l\le C\|(s_1,s_2)-(t_1,t_2)\|^{l/2}.$$

Proof. First of all, we consider

$$\begin{aligned}&\mathbf{E}\|\tilde{\mathbf{X}}_{N,\mathbf{P},\mathbf{q}}(s_1,s_2)-\tilde{\mathbf{X}}_{N,\mathbf{P},\mathbf{q}}(t_1,t_2)\|^l\\&\quad\ll\mathbf{E}(\max\{|\tilde{X}_{N,P_1,q_1}(s_1)-\tilde{X}_{N,P_1,q_1}(t_1)|^l,|\tilde{X}_{N,P_2,q_2}(s_2)-\tilde{X}_{N,P_2,q_2}(t_2)|^l\})\\&\quad\ll\max\{\mathbf{E}|\tilde{X}_{N,P_1,q_1}(s_1)-\tilde{X}_{N,P_1,q_1}(t_1)|^l,\mathbf{E}|\tilde{X}_{N,P_2,q_2}(s_2)-\tilde{X}_{N,P_2,q_2}(t_2)|^l\}.\end{aligned}$$

Now, we use Proposition 2 and hence

$$\begin{aligned}\mathbf{E}\|\tilde{\mathbf{X}}_{N,\mathbf{P},\mathbf{q}}(s_1,s_2)-\tilde{\mathbf{X}}_{N,\mathbf{P},\mathbf{q}}(t_1,t_2)\|^l&\ll\max\{|s_1-t_1|^{l/2},|s_2-t_2|^{l/2}\}\\&\ll\|(s_1,s_2)-(t_1,t_2)\|^{l/2}.\end{aligned}$$

The second part is proved similarly. □

Now, Theorem 3 is a consequence of Prokhorov's Theorem.

4. Proof of Theorem 4

Obviously, it suffices to prove that for every $k \geq 0$

$$\mathbf{E}\left(\max_{0\leq t\leq 1}|X_{N,P}(t)|\right)^k = \mathcal{O}\left(1\right) \tag{4.1}$$

and

$$\mathbf{E}\left(\max_{0\leq t\leq 1}|Y_{N,P}(t)|\right)^k = \mathcal{O}\left(1\right), \tag{4.2}$$

as $N \to \infty$. In a first step, we prove corresponding properties for the truncated processes $\tilde{X}_{N,P}(t)$ and $\tilde{Y}_{N,P}(t)$. In order to shorten our presentation, we will only discuss the process $\tilde{X}_{N,P}(t)$.

Lemma 3. *For every integer $d > 0$ there exists a constant $K > 0$ such that for $\varepsilon > 0$ and $0 < \delta \leq 1$*

$$\nu_N\left(\max_{0\leq s,t\leq 1,|s-t|\leq\delta}|\tilde{X}_{N,P}(s) - \tilde{X}_{N,P}(t)| \geq \varepsilon\right) \leq K\frac{\delta^{d-1}}{\varepsilon^{2d}}.$$

Proof. This property is an immediate consequence of the tightness estimate (of Proposition 2) combined with the arguments of [2, pp. 95]. □

Lemma 4. *For every k, we have uniformly for $0 < \delta \leq 1$*

$$\mathbf{E}\left(\max_{0\leq s,t\leq 1,|s-t|\leq\delta}|\tilde{X}_{N,P}(s) - \tilde{X}_{N,P}(t)|\right)^k = \mathcal{O}\left(\delta^{(k-2)/2}\right).$$

Proof. Set

$$Z_N := \max_{0\leq s,t\leq 1,|s-t|\leq\delta}|\tilde{X}_{N,P}(s) - \tilde{X}_{N,P}(t)|.$$

Furthermore, assume that $2d > k$. Then it follows that

$$\begin{aligned}
\mathbf{E}Z_N^k &= k\int_0^\infty z^{k-1}\nu_N(Z > z)\,dz \\
&= k\int_0^{(K\delta)^{1/2}} z^{k-1}\nu_N(Z > z)\,dz + k\int_{(K\delta)^{1/2}}^\infty z^{k-1}\nu_N(Z > z)\,dz \\
&\leq (K\delta)^{k/2} + kK\delta^{d-1}\int_{(K\delta)^{1/2}}^\infty z^{k-1-2d}\,dz \\
&\ll \delta^{(k-2)/2}
\end{aligned}$$

which proves the lemma. □

Now, observe that the trivial relation

$$\begin{aligned}
\max_{0\leq t\leq 1}|\tilde{X}_{N,P}(t)| &\leq |\tilde{X}_{N,P}(0)| + \max_{0\leq s,t\leq 1,|s-t|\leq 1}|\tilde{X}_{N,P}(s) - \tilde{X}_{N,P}(t)| \\
&= \max_{0\leq s,t\leq 1,|s-t|\leq 1}|\tilde{X}_{N,P}(s) - \tilde{X}_{N,P}(t)|
\end{aligned}$$

combined with Lemma 4 (applied for $\delta = 1$) directly gives

$$\mathbf{E}\left(\max_{0\leq t\leq 1}|\tilde{X}_{N,P}(t)|\right)^k = \mathcal{O}\left(1\right), \tag{4.3}$$

as $N \to \infty$.

In the second step, we compare the moments of $\max|X_{N,P}(t)|$ and $\max|\tilde{X}_{N,P}(t)|$. For this purpose, we make use of the following property of moments.

Lemma 5. *Suppose that U,V are real valued non-negative random variables satisfying $|U-V|\le\varepsilon$ (for some $\varepsilon>0$). Then the k-th moment of U exists if and only if the k-th moment of V exists. More precisely, we have*

$$\mathbf{E}V^k \le \sum_{\ell=0}^{k}\binom{k}{\ell}\varepsilon^\ell\cdot\mathbf{E}U^{k-\ell}. \tag{4.4}$$

Proof. It is of course sufficient to prove (4.4). Therefore notice

$$\mathbf{E}V^k=\mathbf{E}|V-U+U|^k\le\mathbf{E}(|V-U|+|U|)^k$$

and the result follows immediately by the binomial theorem. □

Now, we are ready to complete the proof of Theorem 4. Set

$$U:=\max_{0\le t\le 1}|X_{N,P}(t)|$$

and

$$V:=\max_{0\le t\le 1}|\tilde{X}_{N,P}(t)|.$$

From

$$\max_{0\le t\le 1}|X_{N,P}(t)-\tilde{X}_{N,P}(t)|\ll L^{\eta-\frac12},$$

it follows

$$|U-V|\ll L^{\eta-\frac12},$$

too, and thus, we can combine (4.4) and Lemma 5 to prove (4.1).

As already mentioned the proof of (4.2) is completely the same. Furthermore, it is now an easy exercise to extend the above considerations to the joint case leading to a proof of Theorem 6.

5. The Law of the Iterated Logarithm

Let $q>1$ and $P(x)$ be a polynomial with integer coefficients, degree r, and positive leading term.

First of all, we summarize a few well-known facts about permutation polynomials:

Lemma 6. *$P(x)$ is a permutation polynomial for each power of q if and only if $P(x)$ is a permutation polynomial for q^2. Especially, there are infinitely many polynomials $P(x)$ with integer coefficients and positive leading terms which are permutation polynomials for each power of q.*

Proof. See for instance [15]. □

In order to prove Theorem 7, we follow the approach developed by the third author in [14] and therefore, we have to extend the so called fundamental lemma of [13].

Lemma 7. *Let $P(x)$ be a permutation polynomial for each power of q. Then there is a sequence of independent and identically distributed random variables $(\xi_j)_{0\le j\le L}$ defined on some probability space $(\Omega_N,\mathcal{F}_N,P_N)$ such that*

$$\nu_N\left(s_{q,k}(P(n))\in A\right)=P_N\left(\sum_{j=0}^{k}\xi_j\in A\right)+\frac{2\theta q^{k+1}}{N} \tag{5.1}$$

where $k \le L$ and $|\theta| < 1$ and

$$\nu_N\left(s_{q,L}(P(n)) \in A\right) \le qP_N\left(\sum_{j=0}^{L} \xi_j \in A\right) \tag{5.2}$$

where A is an arbitrary subset of $\mathbb{R}$.

Proof. For the proof, we first of all introduce some notation. For $b_j \in E_q$ $(0 \le j \le k$, $k \le L)$, we set

$$B(b_0, \ldots, b_k) = \{n \in \mathbb{N}_0 | a_{q,j}(P(n)) = b_j, 0 \le j \le k\}.$$

Furthermore, set $\Omega_N := \mathbb{N}_0$ and consider the σ-algebra $\mathcal{F}_N$ generated by

$$\{n \in \mathbb{N}_0 | a_{q,j}(P(n)) = b_j\}, \quad b_j \in E_q, \quad 0 \le j \le L.$$

It is easy to see that each $C \in \mathcal{F}_N$ has a unique representation of the form

$$C = {\bigcup_{(b_0,\ldots,b_L) \in E_q^{L+1}}}' B(b_0, \ldots, b_L) \tag{5.3}$$

where the sum is extended over a subset of E_q^{L+1}. We define P_N as follows

$$P_N(C) := \frac{1}{q^{L+1}} {\sum_{(b_0,\ldots,b_L) \in E_q^{L+1}}}' 1.$$

On this probability space, we introduce a sequence of random variables $(\xi_j), 0 \le j \le L$ defined by

$$\xi_j(n) := a_{q,j}(P(n)), \quad 0 \le j \le L.$$

It follows

$$P_N(\xi_j = b) = \frac{1}{q}, \quad b \in E_q,$$

and moreover

$$P_N(\xi_{i_1} = b_{i_1}, \ldots, \xi_{i_j} = b_{i_j}) = \frac{1}{q^j} = P_N(\xi_{i_1} = b_{i_1}) \cdots P_N(\xi_{i_j} = b_{i_j})$$

where $0 \le i_1 < \ldots < i_j \le L$ and $b_{i_1}, \ldots, b_{i_j} \in E_q$. Therefore the sequence $(\xi_j), 0 \le j \le L$ is independent and identically distributed.

It is clear that the set $\{s_{q,k}(P(n)) \in A\}$ is contained in $\mathcal{F}_N$ for all $k \le L$ and all subsets A of $\mathbb{R}$. Moreover, this set can be written in the form

$$\{s_{q,k}(P(n)) \in A\} = {\bigcup_{(b_0,\ldots,b_k) \in E_q^{k+1}}}' B(b_0, \ldots, b_k)$$

where the sum is extended over a certain subset of E_q^{k+1}. Next, we compute

$$\begin{aligned}\nu_N(s_{q,k}(P(n)) \in A) &= {\sum_{(b_0,\ldots,b_k) \in E_q^{k+1}}}' \nu_N(B(b_0 \ldots, b_k)) \\ &= \frac{1}{N} {\sum_{(b_0,\ldots,b_k) \in E_q^{k+1}}}' \lfloor \frac{N}{q^{k+1}} \rfloor + \delta = \frac{1}{q^{k+1}} {\sum_{(b_0,\ldots,b_k) \in E_q^{k+1}}}' 1 + \frac{2\theta q^{k+1}}{N}\end{aligned}$$

where $\delta \in \{0, 1\}$ and $|\theta| < 1$. If we replace each $(k+1)$-tuple in the last sum by $(b_0, \ldots, b_k, b_{k+1}, \ldots, b_L)$ where $b_j, k < j \le L$ runs through all elements of E_q and replace the factor $1/q^{k+1}$ by $1/q^{L+1}$ then, we don't change the value of the sum. Hence, (5.1) follows.

For the second part, we again have

$$\{s_{q,L}(P(n)) \in A\} = \bigcup_{(b_0,\dots,b_L)\in E_q^{L+1}}{}^{\prime} B(b_0,\dots,b_L)$$

where the sum is extended over a subset of E_q^{L+1}. We consider

$$\begin{aligned}\nu_N(s_{q,L}(P(n)) \in A) &= \sum_{(b_0,\dots,b_L)\in E_q^{L+1}}{}^{\prime} \nu_N(B(b_0,\dots,b_L)) \\ &\le \frac{1}{N} \sum_{(b_0,\dots,b_L)\in E_q^{L+1}}{}^{\prime} 1 \le q\left(\frac{1}{q^{L+1}} \sum_{(b_0,\dots,b_L)\in E_q^{L+1}}{}^{\prime} 1\right)\end{aligned}$$

and the definition of P_N implies (5.2). □

To obtain Theorem 7, we can now proceed as in [14]. Therefore, we give only a sketch of the proof.

Proof of Theorem 7. We consider the stochastic processes $S_{N,k,P}$ together with the truncated versions

$$\tilde{S}_{N,k,P}(t)(n) := \frac{1}{\sigma_q\sqrt{2k\log\log k}}\left(\sum_{j\le J(t)}\left(a_{q,j}(P(n)) - \frac{q-1}{2}\right)\right)$$

where $J(t) = \min\{tk, L-(\log N)^\eta\}$,$t = i/k, i = 0,\dots,k$, and $\eta > 0$. Furthermore, we define

$$Z_{N,k}(t) = \frac{1}{\sigma_q\sqrt{2k\log\log k}}\left(\sum_{j\le tk}\left(\xi_j - \frac{q-1}{2}\right)\right), \quad t = i/k, i = 0,\dots,k$$

for $k \le L$ where the sequence ξ_j is the one of the fundamental lemma and we consider again the truncated versions of these processes

$$\tilde{Z}_{N,k}(t) = \frac{1}{\sigma_q\sqrt{2k\log\log k}}\left(\sum_{j\le J(t)}\left(\xi_j - \frac{q-1}{2}\right)\right), \quad t = i/k, i = 0,\dots,k.$$

First of all (5.2) and Kolmogorov's inequality imply

$$\nu_N\left(\max_{x\le k\le L}\rho(S_{N,k,P},\tilde{S}_{N,k,P}) \ge \epsilon\right) = o(1) \tag{5.4}$$

for all $\epsilon > 0$ and therefore, we need to prove Theorem 7 only for the truncated processes.

By (5.1), we have

$$\nu_N\left(\max_{x\le k\le L}\rho(\tilde{S}_{N,k,P},\mathcal{K}) \ge \epsilon\right) = P_N\left(\max_{x\le k\le L}\rho(\tilde{Z}_{N,k},\mathcal{K}) \ge \epsilon\right) + \mathcal{O}\left(L^{-\eta}\right)$$

and

$$\nu_N\left(\min_{x\le k\le L}\rho(\tilde{S}_{N,k,P},X) < \epsilon\right) = P_N\left(\min_{x\le k\le L}\rho(\tilde{Z}_{N,k},X) < \epsilon\right) + \mathcal{O}\left(L^{-\eta}\right)$$

where $\epsilon > 0$ and $X \in \mathcal{K}$. Hence it is enough to prove the theorem for the processes $\tilde{Z}_{N,k}$.

Using Kolmogorov's inequality once more, we get

$$\nu_N \left(\max_{x \le k \le L} \rho(Z_{N,k}, \tilde{Z}_{N,k}) \ge \epsilon \right) = o(1) \tag{5.5}$$

where $\epsilon > 0$ and because of that it is sufficient to show the theorem for the processes $Z_{N,k}$. But for this processes the theorem is valid by the classical theory. □

The next aim is the proof of Theorem 8. Therefore let $q_1, q_2 > 1$ be integers and $P_1(x), P_2(x)$ polynomials with integer coefficients, degrees $r_1, r_2 \ge 1$ and positive leading terms.

First, we show that part (1) of Theorem 8 is a consequence of Theorem 7. We use the following simple result:

Lemma 8. *Let f_1, f_2 be continues functions on $[0,1]$ and S_1, S_2 subsets of $C[0,1]$. Then there is a constant $C > 0$ depending only on the involved norm such that we have*

$$\rho((f_1, f_2), S_1 \times S_2) \le C\rho(f_1, S_1) + C\rho(f_2, S_2).$$

Proof. First, we consider the case $S_1 = \{g_1\}$ and $S_2 = \{g_2\}$. We have

$$\begin{aligned}
\rho((f_1, f_2), (g_1, g_2)) &= \max_{0 \le t_1, t_2 \le 1} \|(f_1(t_1) - g_1(t_1), f_2(t_2) - g_2(t_2))\| \\
&\le C \max_{0 \le t_1, t_2 \le 1} (\max\{|f_1(t_1) - g_1(t_1)|, |f_2(t_2) - g_2(t_2)|\}) \\
&\le C \max_{0 \le t_1, t_2 \le 1} (|f_1(t_1) - g_1(t_1)| + |f_2(t_2) - g_2(t_2)|) \\
&\le C\rho(f_1, g_1) + C\rho(f_2, g_2).
\end{aligned}$$

The general case follows from the definition of $\rho((f_1, f_2), S_1 \times S_2)$ resp. $\rho(f_i, S_i), i = 1, 2$. □

The proof of part (1) of Theorem 8 runs as follows:

Proof of Theorem 8 (1). Observe that Lemma 8 implies

$$\begin{aligned}
&\nu_N \left(\max_{k_1, k_2 \ge x, k_1 \le L_{q_1}, k_2 \le L_{q_2}} \rho((S_{N,k_1,P_1,q_1}, S_{N,k_2,P_2,q_2}), \mathcal{K}_1) \ge \epsilon \right) \\
&\le \nu_N \left(\left(\max_{x \le k_1 \le L_{q_1}} \rho(S_{N,k_1,P_1,q_1}, \mathcal{K}) \ge \epsilon/C \right) \cup \left(\max_{x \le k_2 \le L_{q_2}} \rho(S_{N,k_2,P_2,q_2}, \mathcal{K}) \ge \epsilon/C \right) \right)
\end{aligned}$$

and

$$\begin{aligned}
&\nu_N \left(\min_{k_1, k_2 \ge x, k_1 \le L_{q_1}, k_2 \le L_{q_2}} \rho((S_{N,k_1,P_1,q_1}, S_{N,k_2,P_2,q_2}), (X_1, X_2)) < \epsilon \right) \\
&\ge \nu_N \left(\left(\min_{x \le k_1 \le L_{q_1}} \rho(S_{N,k_1,P_1,q_1}, X_1) < \epsilon/C \right) \cap \left(\min_{x \le k_2 \le L_{q_2}} \rho(S_{N,k_2,P_2,q_2}, X_2) < \epsilon/C \right) \right).
\end{aligned}$$

By using the simple facts

$$\nu_N(A_1 \cup A_2) \le \nu_N(A_1) + \nu_N(A_2)$$

and

$$\nu_N(A_1 \cap A_2) \ge \nu_N(A_1) + \nu_N(A_2) - 1$$

where A_1, A_2 are arbitrary subsets of $\mathbb{N}_0$ the result follows. □

For the proof of the second part of Theorem 8, we prove a two dimensional version of the fundamental lemma. (Till the end of the section, we use the notation $L := L_{q_1 q_2}$.)

Lemma 9. *Let $(q_1, q_2) = 1$ and $P_i(x)$ be permutation polynomials for each power of q_i, $i = 1, 2$. Then there are independent random variables $(\xi_j)_{0 \le j \le L}, (\eta_j)_{0 \le j \le L}$ where the ξ_j resp. η_j are identically distributed defined on some probability space $(\Omega_N, \mathcal{F}_N, P_N)$ such that we have*

$$\nu_N((s_{q_1,k}(P_1(n)), s_{q_2,k}(P_2(n))) \in A) = P_N\left(\sum_{j=0}^{k} (\xi_j, \eta_j) \in A\right) + \frac{2\theta (q_1 q_2)^{k+1}}{N} \tag{5.6}$$

where $k \le L$ and $|\theta| < 1$ and

$$\nu_N((s_{q_1,L}(P_1(n)), s_{q_2,L}(P_2(n))) \in A) \le q_1 q_2 P_N\left(\sum_{j=0}^{L} (\xi_j, \eta_j) \in A\right) \tag{5.7}$$

where A is an arbitrary subset of $\mathbb{R}^2$.

Proof. We are going to use the following notation. Let $b_j^{(i)}, 0 \le j \le k, i = 1, 2$ with $b_j^{(i)} \in E_{q_i}$ be given. Then, we write

$$B(b_0^{(1)}, \ldots, b_k^{(1)}; b_0^{(2)}, \ldots, b_k^{(2)}) = \{n \in \mathbb{N}_0 | a_{q_i,j}(P_i(n)) = b_j^{(i)}, 0 \le j \le k, i = 1, 2\}.$$

We define $\Omega_N := \mathbb{N}_0$ and consider the σ-algebra $\mathcal{F}_N$ generated by

$$\{n \in \mathbb{N}_0 | a_{q_i,j}(P_i(n)) = b_j\}, \quad b_j \in E_{q_i}, \quad 0 \le j \le L, i = 1, 2.$$

As in the proof of Lemma 7 each $C \in \mathcal{F}_N$ has a unique representation of the form

$$C = \bigcup_{(b_0^{(i)}, \ldots, b_L^{(i)}) \in E_{q_i}^{L+1}, i=1,2}{}' B(b_0^{(1)}, \ldots, b_L^{(1)}; b_0^{(2)}, \ldots, b_L^{(2)})$$

where the sum is extended over a subset of $E_{q_1}^{L+1} \times E_{q_2}^{L+1}$. Therefore, we define P_N by

$$P_N(C) := \frac{1}{(q_1 q_2)^{L+1}} \sum_{(b_0^{(i)}, \ldots, b_L^{i}) \in E_{q_{(i)}}^{L+1}, i=1,2}{}' 1.$$

On this probability space, we consider the following random variables

$$\xi_j(n) := a_{q_1,j}(P_1(n)), \quad 0 \le j \le L$$

and

$$\eta_j(n) := a_{q_2,j}(P_2(n)), \quad 0 \le j \le L.$$

As in the proof of Lemma 7 it follows that the random variables are independent and the ξ_j resp. η_j are identically distributed with

$$P_N(\xi_j = b) = \frac{1}{q_1}, \quad b \in E_{q_1},$$

and

$$P_N(\eta_j = b) = \frac{1}{q_2}, \quad b \in E_{q_2}.$$

If we write

$$\{(s_{q_1,k}(P_1(n)),s_{q_2,k}(P_2(n))) \in A\} = \bigcup_{(b_0^{(i)},\dots,b_k^{(i)})\in E_{q_i}^{k+1}, i=1,2}{}^{\prime} B(b_0^{(1)},\dots,b_k^{(1)};b_0^{(2)},\dots,b_k^{(2)})$$

where the sum is extended over a suitable subset of $E_{q_1}^{k+1}\times E_{q_2}^{k+1}$ and note that because of the Chinese remainder theorem

$$\nu_N(B(b_0^{(1)},\dots,b_k^{(1)};b_0^{(2)},\dots,b_k^{(2)})) = \frac{1}{N}\left(\lfloor \frac{N}{(q_1q_2)^{k+1}}\rfloor + \delta\right)$$

where $\delta\in\{0,1\}$ then (5.6) and (5.7) follow in a similar way as in the proof of Lemma 7. □

With this Lemma, we can reduce the proof of part (2) of Theorem 8 to the case of independent and identically distributed random variables.

Proof of Theorem 8 (2). We introduce the notation

$$\mathbf{S}_{N,k,\mathbf{P},\mathbf{q}} := (S_{N,k,P_1,q_1}, S_{N,k,P_2,q_2})$$

and

$$\tilde{\mathbf{S}}_{N,k,\mathbf{P},\mathbf{q}} := (\tilde{S}_{N,k,P_1,q_1}, \tilde{S}_{N,k,P_2,q_2})$$

where $\mathbf{P}:=(P_1,P_2)$, $\mathbf{q}:=(q_1,q_2)$ and $\tilde{S}_{N,k,P_1,q_1}$ is the truncated process defined in the proof of the first part of Theorem 8.

We also consider the processes $Z_{N,k}(t)$ resp. $\tilde{Z}_{N,k}(t)$ defined in the proof of Theorem 8 for the random variables ξ_j of the fundamental lemma and denote by $W_{N,k}(t)$ resp. $\tilde{W}_{N,k}(t)$ the corresponding processes for the random variables η_j of the fundamental lemma. Furthermore, we set

$$\mathbf{Z}_{N,k}(t) := (Z_{N,k}(t), W_{N,k}(t))$$

and

$$\tilde{\mathbf{Z}}_{N,k}(t) := (\tilde{Z}_{N,k}(t), \tilde{W}_{N,k}(t)).$$

First of all, we can conclude from Lemma 8 that

$$\nu_N(\max_{x\le k\le L}\rho(\mathbf{S}_{N,k,\mathbf{P},\mathbf{q}},\tilde{\mathbf{S}}_{N,k,\mathbf{P},\mathbf{q}})\ge\epsilon) \le \nu_N((\max_{x\le k\le L}\rho(S_{N,k,P_1,q_1},\tilde{S}_{N,k,P_1,q_1})\ge\epsilon/C) \cup (\max_{x\le k\le L}\rho(S_{N,k,P_2,q_2},\tilde{S}_{N,k,P_2,q_2})\ge\epsilon/C)).$$

By combining this with (5.4) it follows that it is enough to prove the theorem for the truncated processes.

Now, the fundamental lemma implies

$$\nu_N(\max_{x\le k\le L}\rho(\tilde{\mathbf{S}}_{N,k,\mathbf{P},\mathbf{q}},\mathcal{K}_2)\ge\epsilon) = P_N(\max_{x\le k\le L}\rho(\tilde{\mathbf{Z}}_{N,k},\mathcal{K}_2)\ge\epsilon) + \mathcal{O}\left(L^{-\eta}\right)$$

and

$$\nu_N(\min_{x\le k\le L}\rho(\tilde{\mathbf{S}}_{N,k,\mathbf{P},\mathbf{q}},(X_1,X_2))<\epsilon) = P_N(\min_{x\le k\le L}\rho(\tilde{\mathbf{Z}}_{N,k},(X_1,X_2))<\epsilon)+\mathcal{O}\left(L^{-\eta}\right)$$

where $\epsilon>0$ and $(X_1,X_2)\in\mathcal{K}_2$. Therefore, it is sufficient to prove the iterated logarithm law of the form given in Theorem 8 (2) for the processes $\tilde{\mathbf{Z}}_{N,k}$.

Using once more Lemma 8 together with (5.5), we can further reduce the proof to the processes $\mathbf{Z}_{N,k}$. But for these processes Theorem 8 (2) is true by the classical law of iterated logarithm due to Strassen (see [18]). □

6. Generalizations

In this section, we shortly outline generalizations of the results of the paper to more general q-additive functions. We only state a possible extension of Theorem 3, all other Theorems can be extended in a similar way.

We consider a sequence of q-additive functions

$$f_N(n) := \sum_{j\ge 0} f_{N,j}(a_{q,j}(n)) \tag{6.1}$$

where $f_{N,j}(a), N \ge 1, j \ge 0, a \in E_q$, is a family of real numbers with the property $f_{N,j}(0) = 0$ for all N and j. Using partial sums of (6.1), we construct a model of the Brownian motion generalizing that given in Theorem 3. Our result is an analogue of Theorem 5.2 in [13].

In order to state the result, we need some notation. Set

$$\bar{f}_{N,j}(a) = f_{N,j}(a) - \frac{1}{q}\sum_{b=0}^{q-1} f_{N,j}(b), \qquad \sigma_{N,j}^2 = \frac{1}{q}\sum_{a=0}^{q-1} \bar{f}_{N,j}(a)^2,$$

$$B_{N,k}^2 = \sum_{j\le k} \sigma_{N,j}^2, \qquad B_N^2 = B_{N,rL}^2$$

where $r \ge 1$. With

$$y(t) := y_N(t) = \max\{k : \ B_{N,k}^2 \le tB_N^2\}, \quad 0 \le t \le 1,$$

we can formulate the following generalization of Theorem 3.

Theorem 9. *Let $q \ge 2$ and $P(x)$ be an integer polynomial of degree $r \ge 1$ with positive leading term. If the sequence of additive functions f_N satisfies the following conditions, as $N \longrightarrow \infty$,*

$$\max_{j\le rL}\max_{a\in E_q} |f_{N,j}(a)| = o(1), \tag{6.2}$$

$$\sum_{\substack{j \le (\log N)^\eta or \\ rL-(\log N)^\eta < j \le rL}} \max_{a\in E_q} |f_{N,j}(a)| = o(1) \tag{6.3}$$

where $\eta > 0$, and

$$B_N = 1 + O(1), \tag{6.4}$$

then the process

$$H_{N,P}(t)(n) := \sum_{j\le y(t)} \bar{f}_{N,j}(a_{q,j}(P(n)))$$

(where t is a point of discontinuity of the function $y(t)$) weakly converges to the Brownian motion.

Proof. Let $\xi_{N,j}, 1 \le N, j \le rL$ be independent random variables for each fixed N given by

$$P(\xi_{N,j} = \bar{f}_{N,j}(a)) = \frac{1}{q}, \quad a = 0, 1, \dots, q-1$$

and

$$Z_N(t) = \sum_{j \le y(t)} \xi_{N,j}, \quad 0 \le t \le 1.$$

According to a well known result of Prokhorov (and by the assumptions of Theorem 9) Z_N weakly converges to the Brownian motion. By using this result instead of Donsker's theorem and the method of the proof of Theorem 3, we immediately obtain the result. □

Remark 1. Condition (6.2) actually means infinitesimality of the summands. However, one cannot expect much more by using Lindeberg's condition instead of it (see the comments in [13]). Condition (6.3) is needed to deal with polynomials while (6.4) comes from Prokhorov's paper.

Remark 2. As already mentioned, Theorem 9 is a generalization of Theorem 3. We only have to set

$$f_N(n) = \frac{1}{\sigma_q \sqrt{rL}} s_q(n).$$

References

[1] N. L. Bassily and I. Kátai, Distribution of the Values of q-Additive Functions on Polynomial Sequences, Acta Math. Hung., 68 (1995), 353-361.

[2] P. Billingsley, Convergence of Probability Measures, John Wiley & Sons, 2. ed., (New York, 1999).

[3] J. Coquet, Corrélation de suites arithmétiques, Sémin. Delange-Pisot-Poitou 20e Année 1978/79, Exp. 15 (1980), 12 p.

[4] H. Delange, Sur les fonctions q-additives ou q-multiplicatives, Acta Arith., 21 (1972), 285-298.

[5] H. Delange, Sur la fonction sommatoire de la fonction "Somme de Chiffres", L'Enseignement math., 21 (1975), 31-77.

[6] M. Drmota, The Joint Distribution of q-Additive Functions, Acta Arith., 100 (2001), 17-39.

[7] M. Drmota and J. Gajdosik, The Distribution of the Sum-of-Digits Function, J. Theor. Nombres Bordx., 10 (1998), 17-32.

[8] M. Drmota and W. Steiner, The Zeckendorf Expansion of Polynomial Sequences, J. Theor. Nombres Bordx., submitted.

[9] P. J. Grabner, P. Kirschenhofer, H. Prodinger, and R. F. Tichy, On the Moments of the Sum-of-Digits Function, Applications of Fibonacci Numbers, 5 (1993), 263-271.

[10] I. Kátai, Distribution of q-Additive Function, Probability Theory and Applications, Essays to the Mem. of J. Mogyorodi, Math. Appl., Kluwer, Dortrecht, 80 (1992), 309-318.

[11] D.-H. Kim, On the Joint Distribution of q-Additive Functions in Residue Classes, J. Number Theory, 74 (1999), 307-336.

[12] M. Loève, Probability Theory, D. Van Nostrand Company, (Princeton, 1963).

[13] E. Manstavičius, Probabilistic Theory of Additive Functions related to Systems of Numerations, Analytic and Probabilistic Methods in Number Theory, VSP, (Utrecht 1997), 413-430.

[14] E. Manstavičius, Sums of Digits obey the Strassen Law, Proceedings of the 38-th Conference of the Lithuanian Mathematical Society, R.Ciegis et al (Eds), Technika, (Vilnius, 1997), 33-38.

[15] W. Nöbauer, Über Prermutationspolynome und Permutationsfunktionen für Primzahlpotenzen, Monatshefte Mathematik, 69 (1965), 230-238.

[16] D. Revuz and M. Yor, Continuous Martingales and Brownian Motion, 3. ed., Springer, (Berlin 1999).

[17] W. Steiner, On the Joint Distribution of q-Additive Functions on Polynomial Sequences, Proceedings of the Conference dedicated to the 90th Anniversary of B. V. Gnedenko, submitted.

[18] V. Strassen, An Invariance Principle for the Law of the Iterated Logarithm, Z. für Wahrscheinlichkeitstheorie und Verw. Gebiete, 3 (1964), 211-226.

Michael Drmota
Vienna University of Technology, Department of Geometry,
Wiedner Hauptstraße 8-10/113,
A-1040 Vienna, Austria,

Michael Fuchs
Vienna University of Technology, Department of Geometry,
Wiedner Hauptstraße 8-10/113,
A-1040 Vienna, Austria,

Eugenijus Manstavičius
Vilnius University, Department of Mathematics and Informatics,
Naugarduko str. 24,
LT 2600, Vilnius, Lithuania.