On the law of the iterated logarithm for random exponential sums

István Berkes* and Bence Borda†

Abstract

The asymptotic behavior of exponential sums $\sum_{k=1}^N \exp(2\pi i n_k \alpha)$ for Hadamard lacunary (n_k) is well known, but for general (n_k) very few precise results exist, due to number theoretic difficulties. It is therefore natural to consider random (n_k) and in this paper we prove the law of the iterated logarithm for $\sum_{k=1}^N \exp(2\pi i n_k \alpha)$ if the gaps $n_{k+1} - n_k$ are independent, identically distributed random variables. As a comparison, we give a lower bound for the discrepancy of $\{n_k \alpha\}$ under the same random model, exhibiting a completely different behavior.

1 Introduction

It is well known that the behavior of lacunary series resembles that of independent random variables. The following classical result was proved by Erdős and Gál [8].

Theorem. *Let (n_k) be a sequence of positive numbers satisfying*

$$n_{k+1}/n_k \geq q > 1 \qquad k = 1, 2, \ldots . \tag{1.1}$$

Then

$$\limsup_{N\to\infty} \frac{\left|\sum_{k=1}^N e^{2\pi i n_k x}\right|}{\sqrt{N \log\log N}} = 1 \qquad \textit{for almost all } x. \tag{1.2}$$

*A. Rényi Institute of Mathematics, 1053 Budapest, Reáltanoda u. 13-15, Hungary. e-mail: berkes.istvan@renyi.mta.hu. Research supported by FWF Grant P24302-N18 and NKFIH grant K 108615.

†A. Rényi Institute of Mathematics, 1053 Budapest, Reáltanoda u. 13-15, Hungary. e-mail: bordabence85@gmail.com

Note that here the n_k need not be integers. As was shown by Takahashi [23], [24], for integer n_k the gap condition (1.1) can be weakened and an optimal condition was obtained by Berkes [4]: relation (1.2) remains valid if n_k are positive integers and

$$n_{k+1}/n_k \geq 1 + (\log\log k)^\gamma/\sqrt{k}, \qquad \gamma > 1/2$$

for $k \geq k_0$ and this becomes false for $\gamma = 1/2$. In particular, there exist sequences $n_k \geq e^{\sqrt{k}}$ such that (1.2) is not true. This does not mean, however, that for sequences (n_k) growing at a slower speed, (1.2) cannot be true. From the results of Salem and Zygmund [20] it follows that there exists a sequence (n_k) of integers with $n_k = O(k)$ such that (1.2) holds, and Aistleitner and Fukuyama [2] showed the existence of an integer sequence (n_k) with $n_{k+1} - n_k = O(1)$ satisfying (1.2). For other, related constructions see [1], [3], [11], [12], [15]. Note, however, that all these constructions use random (n_k) and no explicit polynomially growing (n_k) satisfying (1.2) seems to be known. Indeed, proving (1.2) for a "concrete" sequence (n_k) requires precise estimates for the number of solutions of the Diophantine equation

$$\pm n_{k_1} \pm \ldots \pm n_{k_r} = M, \qquad 1 \leq k_1, \ldots, k_r \leq N \tag{1.3}$$

which is a notoriously difficult problem of additive number theory, see e.g. Halberstam and Roth [13], Chapters II and III. Thus proving precise asymptotic results for exponential sums $\sum_{k=1}^N \exp(2\pi i n_k x)$ is more or less restricted to random sequences (n_k), and the purpose of the present paper is to study the law of the iterated logarithm in the random case.

Naturally, there are many different types of random sequences; we will consider the simplest case when the gaps $n_{k+1} - n_k$ are independent, identically distributed (i.i.d.) random variables. As in [8], we will not assume that the n_k are integers, although, as we will see, this is the most interesting case. We will not assume, either, that the sequence (n_k) is increasing. To avoid confusion between random and nonrandom sequences, in the random case the sequence (n_k) will be denoted by (S_k); the assumption that the gaps $S_{k+1} - S_k$ are i.i.d. means that $S_k = \sum_{j=1}^k X_j$ is a random walk. Schatte [22] showed that in the case when X_1 is absolutely continuous, for any fixed x the sequence $\{S_k x\}$ (where $\{\cdot\}$ denotes fractional part) has strong independence properties implying the LIL for the discrepancy of $\{S_k x\}$.

For the same class of random walks, the almost everywhere convergence of $\sum_{k=1}^{\infty} c_k f(S_k x)$ under $\sum_{k=1}^{\infty} c_k^2 < +\infty$ where f is a smooth periodic function was proved in Berkes and Weber [6], Theorem 4.2. Whether this remains valid for integer valued (n_k) remains open; for a partial result see [6], Theorem 4.3. Upper bounds for the discrepancy of $\{S_k x\}$, which is closely related to the behavior of the corresponding exponential sum, are given in Weber [25] and Berkes and Weber [6]; the bounds depend on the distribution of the variable X_1 defining the random walk and on the rational approximation properties of x. Improving the tools in [6], [25] and determining the precise asymptotics of high moments of the exponential sum $\sum_{k=1}^{n} \exp(2\pi i S_k x)$, in this paper we will prove the law of the iterated logarithm for the exponential sum for arbitrary random walks (S_n).

Theorem 1.1. *Let $X_1, X_2, \ldots$ be i.i.d. random variables with characteristic function φ, let $S_k = \sum_{j=1}^{k} X_j$, and let $\alpha \in \mathbb{R}$. Suppose that $\exp(2\pi i X_1 \alpha)$ is non-degenerate.*

(i) If $\mathbb{P}(2X_1\alpha \in \mathbb{Z}) < 1$, then with probability 1

$$\limsup_{n\to\infty} \frac{1}{\sqrt{n \log\log n}} \left| \sum_{k=1}^{n} e^{2\pi i S_k \alpha} \right| = \frac{\sqrt{1 - |\varphi(2\pi\alpha)|^2}}{|1 - \varphi(2\pi\alpha)|}. \tag{1.4}$$

(ii) If $\mathbb{P}(2X_1\alpha \in \mathbb{Z}) = 1$, then with probability 1

$$\limsup_{n\to\infty} \frac{1}{\sqrt{n \log\log n}} \left| \sum_{k=1}^{n} e^{2\pi i S_k \alpha} \right| = \sqrt{2}\frac{\sqrt{1 - |\varphi(2\pi\alpha)|^2}}{|1 - \varphi(2\pi\alpha)|}. \tag{1.5}$$

Note that the variable x in the sum $\sum_{k=1}^{N} \exp(2\pi i S_k x)$ was replaced by α to emphasize that, unlike in (1.2), in (1.4) α is fixed and and the relation holds with probability 1 in the space of the random walk (S_k). From now on, we will use the abbreviation "a.s." (almost surely) instead of "with probability 1".

If $\exp(2\pi i X_1 \alpha)$ is degenerate, i.e. if there exists a constant $c \in \mathbb{C}$ such that $\exp(2\pi i X_1 \alpha) = c$ a.s., then $\exp(2\pi i S_k \alpha) = c^k$ a.s. In this case clearly no law of the iterated logarithm with a nonzero limsup can hold for for $\exp(2\pi i S_k \alpha)$. Note that $\exp(2\pi i X_1 \alpha)$ is degenerate

if and only if $\mathbb{P}((X_1 - X_2)\alpha \in \mathbb{Z}) = 1$, or alternatively if and only if $|\varphi(2\pi\alpha)| = 1$.

A random variable X_1 is called a lattice variable if there exist $a, b \in \mathbb{R}$ such that $X_1 \in a+b\mathbb{Z}$ a.s. If X_1 is not a lattice variable (e.g. if it has a continuous distribution), then for any $\alpha \neq 0$ the random variable $\exp(2\pi i X_1 \alpha)$ is non-degenerate, moreover we have $\mathbb{P}(2X_1\alpha \in \mathbb{Z}) < 1$, and thus (1.4) holds.

In the case of a lattice variable X_1 there are only countably many exceptional values of α for which $\exp(2\pi i X_1 \alpha)$ is degenerate. Even though the law of the iterated logarithm holds whenever $\exp(2\pi i X_1 \alpha)$ is non-degenerate, the structure of the sequence $\exp(2\pi i S_k \alpha)$ can be very different for different values of α. For example, if X_1 is integer valued and non-degenerate, and α is irrational, then the possible values of the sequence $\exp(2\pi i S_k \alpha)$ form a countable dense subset of the unit circle, while for rational α the corresponding set is finite (in fact comprised of certain roots of unity). The law of the iterated logarithm in the last case follows relatively easily from Markov chain theory, in contrast to the case of a non-lattice X_1, which lies considerably deeper.

Note that the condition $\mathbb{P}(2X_1\alpha \in \mathbb{Z}) = 1$ in (ii) is equivalent to $\exp(2\pi i X_1 \alpha) = \pm 1$ a.s. In this case the terms $\exp(2\pi i S_k \alpha)$ of the random exponential sum are all ± 1 a.s. If, on the other hand $\mathbb{P}(2X_1\alpha \in \mathbb{Z}) < 1$, then the terms are not all purely real.

It is interesting to note that in Theorem 1.1 no assumptions were made about the moments of $|X_1|$ and the distribution of X_1 enters the theorem only through arithmetic conditions on $(X_1 - X_2)\alpha$ and $2X_1\alpha$. The moments of $|X_1|$, or more generally, the tail behavior of $|X_1|$, influences only the growth of the sequence $|S_n|$. Assume for example that

$$\mathbb{P}(|X_1| > t) \sim ct^{-\beta} \quad \text{as } t \to \infty \tag{1.6}$$

for some $c > 0$, $0 < \beta < 2$. Then $\mathbb{E}|X_1|^\gamma$ is finite for $\gamma < \beta$ and infinite for $\gamma > \beta$ and by classical results of probability theory (see e.g. Feller [9], p. 580, Lévy [17], p. 143) $S_n/n^{1/\beta}$ has a non-degenerate limit distribution with characteristic function $\exp(-c_1|t|^\beta)$, and

$$|S_n| = O(n^{1/\beta+\varepsilon}) \qquad \text{a.s.}$$

holds for $\varepsilon > 0$, but not for $\varepsilon < 0$. Hence in this case S_k has polynomial growth. The case $\beta = 1/2$ is of particular interest, since the corresponding nonrandom sequence $n_k = k^2$ is the only "concrete" polynomial case when the precise asymptotics of the exponential sum

$\sum_{k=1}^{N} \exp(2\pi i n_k \alpha)$ is known. In this case Fiedler, Jurkat and Körner [10] showed that given any positive nondecreasing function $g(n)$, for almost all α the relation

$$\sum_{k=1}^{n} \exp(2\pi i k^2 \alpha) \ll \sqrt{n} g(n) \tag{1.7}$$

holds if and only if

$$\sum_{n=1}^{\infty} \frac{1}{n g^4(n)} = \infty.$$

In particular, (1.7) holds if $g(n) = (\log n)^{1/4+\varepsilon}$ for $\varepsilon > 0$, but not for $\varepsilon = 0$. Also, if (1.7) holds with some $g(n)$, then it also holds for $cg(n)$ for any $c > 0$ and thus for $\sum_{k=1}^{n} \exp(2\pi i k^2 \alpha)$ no law of the iterated logarithm type result can hold. As Hardy and Littlewood [14] showed, for fixed α the behavior of the sum is connected to the rational approximation properties of α. We stress, however, that in the random case exhibiting the same growth of (S_k), the LIL holds for $\sum_{k=1}^{N} \exp(2\pi i S_k \alpha)$.

In view of Koksma's inequality (see [16], p. 143), under the assumptions of Theorem 1.1 the discrepancy $D_N(\{S_k\alpha\})$ of the first N terms of the sequence $\{S_k\alpha\}$ satisfies with probability 1

$$D_N(\{S_k\alpha\}) \gg N^{-1/2}(\log\log N)^{1/2}$$

for infinitely many N. By the results of Schatte [22], for absolutely continuous X_1 this estimate is sharp, but as the remark at the end of our paper will show, if X_1 is integer valued, has mean 0 and finite variance and

$$\left|\alpha - \frac{p}{q}\right| < \frac{C}{q^\gamma} \tag{1.8}$$

for infinitely many rationals p/q with some constants $C > 0$ and $\gamma > 2$, then with probability 1 we have

$$D_N(\{S_k\alpha\}) \gg N^{-1/(2\gamma-2)-\varepsilon}$$

for any $\varepsilon > 0$ and infinitely many N. Thus for irrational numbers α allowing a very good approximation with rational numbers, the order of magnitude of the discrepancy can be much greater than $N^{-1/2}(\log\log N)^{1/2}$. In the opposite direction, Weber [25] proved that

$$D_N(\{S_k\alpha\}) \ll N^{-1/(\gamma-1)+\varepsilon} \qquad \text{a.s.}$$

for any $\varepsilon > 0$. The precise order of magnitude of $D_N(\{S_k\alpha\})$ remains open.

2 A moment estimate

We use $\|x\|$ to denote the distance of a real number x from the nearest integer. Recall that $\|-x\| = \|x\|$ and $\|x+y\| \leq \|x\| + \|y\|$ for any $x, y \in \mathbb{R}$. We will also frequently use the fact that the characteristic function φ of an arbitrary distribution satisfies $\varphi(-x) = \bar{\varphi}(x)$ and $|\varphi(x)| \leq 1$ for any $x \in \mathbb{R}$.

First, we find a simple upper bound for $|\varphi|$.

Proposition 2.1. *Let X_1, X_2 be independent random variables with characteristic function φ. For any $t \in \mathbb{R}$ we have*

$$1 - |\varphi(\pi t)| \geq \left(\mathbb{E}\,\|t(X_1 - X_2)\|\right)^2.$$

Proof. Since X_1, X_2 are independent, we have

$$\mathbb{E}e^{\pi i t(X_1 - X_2)} = \mathbb{E}e^{\pi i t X_1}\mathbb{E}e^{-\pi i t X_2} = |\varphi(\pi t)|^2$$

for any $t \in \mathbb{R}$. After taking the real part, and using $|\varphi| \leq 1$ we obtain

$$1 - |\varphi(\pi t)| \geq \frac{1 - |\varphi(\pi t)|^2}{2} = \mathbb{E}\frac{1 - \cos(\pi t(X_1 - X_2))}{2}.$$

Let us now use the general estimate

$$\frac{1 - \cos(\pi x)}{2} \geq \frac{\sin^2(\pi x)}{4} \geq \|x\|^2,$$

valid for all $x \in \mathbb{R}$, to get

$$1 - |\varphi(\pi t)| \geq \mathbb{E}\,\|t(X_1 - X_2)\|^2.$$

Applying Jensen's inequality finishes the proof.

□

The following result, giving a sharp asymptotic bound for the high moments of $\sum_{k=1}^{n} \exp(2\pi i S_k \alpha)$, is the crucial ingredient of the proof of Theorem 1.1.

Proposition 2.2. *Let $X_1, X_2, \ldots$ be i.i.d. random variables with characteristic function φ, and let $S_k = \sum_{j=1}^{k} X_j$. Let $\alpha \in \mathbb{R}$ be such that*

$$\mathbb{P}\left(4\alpha(X_1 - X_2) \in \mathbb{Z}\right) < 1, \tag{2.1}$$

and let

$$R = \frac{16}{\left(\mathbb{E}\,\|4\alpha(X_1 - X_2)\|\right)^2}.$$

For any integers $p \geq 1$, $m \geq 0$ and $n \geq 1$ we have

$$\left| \mathbb{E} \left| \sum_{k=m+1}^{m+n} e^{2\pi i S_k \alpha} \right|^{2p} - \left(\frac{1 - |\varphi(2\pi\alpha)|^2}{|1 - \varphi(2\pi\alpha)|^2} \right)^p p!^2 \binom{n}{p} \right| \leq$$

$$(2pR)^{2p} \max_{0<q<p} \frac{q^{2p-q} n^q}{q! R^{q-1}} + (pR)^{p+1} n^{p-1}.$$

Note that assumption (2.1) is stronger than the nondegeneracy condition in Theorem 1.1 and implies that

$$\mathbb{E}\,\|4\alpha(X_1 - X_2)\| > 0.$$

If (2.1) fails then, as we will see, $\{e^{2\pi i S_k \alpha}, k \geq 1\}$ is an exponentially mixing Markov chain and Theorem 1.1 can be deduced from the theory of mixing processes.

Proof. Expanding the power we get

$$\mathbb{E} \left| \sum_{k=m+1}^{m+n} e^{2\pi i S_k \alpha} \right|^{2p} = \sum_{m+1 \leq \ell_1, \ldots, \ell_{2p} \leq m+n} \mathbb{E} e^{2\pi i \alpha \left(S_{\ell_1} - S_{\ell_2} + \cdots + S_{\ell_{2p-1}} - S_{\ell_{2p}} \right)}. \tag{2.2}$$

Let $[2p] = \{1, 2, \ldots, 2p\}$. We call $B = (B_1, \ldots, B_s)$ an ordered partition of $[2p]$ if $B_1, \ldots, B_s$ are pairwise disjoint, nonempty subsets of $[2p]$ the union of which is $[2p]$. For any $2p$-tuple $\ell = (\ell_1, \ldots, \ell_{2p})$ let us define an ordered partition $B(\ell)$ of $[2p]$ the following way. If

$$\{\ell_1, \ldots, \ell_{2p}\} = \{k_1, \ldots, k_s\} \tag{2.3}$$

with $k_1 < \cdots < k_s$, then let

$$B_j(\ell) = \{i \in [2p] \ : \ \ell_i = k_j\},$$

and $B(\ell) = (B_1(\ell), \ldots, B_s(\ell))$. We will estimate the sum of the terms in (2.2) for which $B(\ell)$ is a given ordered partition B of $[2p]$. Let us thus introduce the notation

$$\Sigma(B) = \sum_{\substack{m+1\le \ell_1,\dots,\ell_{2p}\le m+n \\ B(\ell)=B}} \mathbb{E}e^{2\pi i\alpha\left(S_{\ell_1}-S_{\ell_2}+\cdots+S_{\ell_{2p-1}}-S_{\ell_{2p}}\right)}.$$

Fix an ordered partition $B = (B_1, \dots, B_s)$, and let ℓ be such that $B(\ell) = B$. Let $k_1 < \cdots < k_s$ be as in (2.3). Then

$$S_{\ell_1} - S_{\ell_2} + \cdots + S_{\ell_{2p-1}} - S_{\ell_{2p}} = \varepsilon_1 S_{k_1} + \cdots + \varepsilon_s S_{k_s},$$

where $\varepsilon_1, \dots, \varepsilon_s$ are integers depending only on B, in fact

$$\varepsilon_j = \sum_{i\in B_j} (-1)^{i+1} \tag{2.4}$$

for all $1 \le j \le s$. Let $q = q(B)$ denote the maximum number of nonempty intervals $I_1, \dots, I_q$ partitioning $[s]$ such that $\sum_{j\in I_k} \varepsilon_j = 0$ for every $1 \le k \le q$. From (2.4) we obtain that whenever $I \subseteq [s]$ is a nonempty interval such that $\sum_{j\in I} \varepsilon_j = 0$, then

$$\sum_{i\in \cup_{j\in I} B_j} (-1)^{i+1} = 0.$$

Thus $\cup_{j\in I} B_j$ contains both an even and an odd integer in $[2p]$, and so its cardinality is at least 2. Since B is a partition of $[2p]$, we have

$$2q \le \sum_{k=1}^{q} |\cup_{j\in I_k} B_j| = \sum_{j=1}^{s} |B_j| = 2p.$$

Hence $q \le p$. Moreover, we have $q = p$ if and only if there exists a partition of $[s]$ into nonempty intervals $I_1, \dots, I_p$ such that $\cup_{j\in I_k} B_j$ contains precisely one even and one odd integer for every $1 \le k \le p$.

We first compute $\Sigma(B)$ in the case $q = p$, which, as we will see, gives the main contribution. Let π_e and π_o be arbitrary permutations of the even and odd integers in $[2p]$, respectively, and let $\sigma \in \{-1, 0, 1\}^p$ also be arbitrary. Let us construct an ordered partition $B = B(\pi_e, \pi_o, \sigma) = (B_1, \dots, B_s)$ of $[2p]$ in exactly p steps the following way. In the first step consider $\pi_o(1), \pi_e(2)$. If $\sigma_1 = -1$, then let $B_1 = \{\pi_o(1)\}$ and $B_2 = \{\pi_e(2)\}$. If $\sigma_1 = 1$, then let $B_1 = \{\pi_e(2)\}$ and $B_2 = \{\pi_o(1)\}$. If $\sigma_1 = 0$, then let $B_1 = \{\pi_o(1), \pi_e(2)\}$. We proceed in a similar way. In step k we add the sets $\{\pi_o(2k-1)\}$ and $\{\pi_e(2k)\}$, or

$\{\pi_e(2k)\}$ and $\{\pi_o(2k-1)\}$, or $\{\pi_o(2k-1), \pi_e(2k)\}$ to the end of the list of previously chosen sets, depending on whether $\sigma_k = -1, 1$, or 0.

It is easy to see that for an ordered partition B of $[2p]$ we have $q = p$ if and only if $B = B(\pi_e, \pi_o, \sigma)$ for some π_e, π_o, σ as above. Indeed, the desired partition of $[s]$ into intervals $I_1, \ldots, I_p$ is that I_k is the set of indices of $(B_1, \ldots, B_s)$ chosen in step k of the construction. In particular there are exactly $p!^2 3^p$ ordered partitions B for which $q = p$.

Fix π_e, π_o, σ as above, let $B = B(\pi_e, \pi_o, \sigma)$, and consider $\Sigma(B)$. For any $1 \leq k \leq p$ let $m_k = \min\left\{\ell_{\pi_o(2k-1)}, \ell_{\pi_e(2k)}\right\}$ and $M_k = \max\left\{\ell_{\pi_o(2k-1)}, \ell_{\pi_e(2k)}\right\}$. Note that

$$m + 1 \leq m_1 \leq M_1 < m_2 \leq M_2 < \cdots < m_p \leq M_p \leq m + n, \quad (2.5)$$

$$S_{\ell_1} - S_{\ell_2} + \cdots + S_{\ell_{2p-1}} - S_{\ell_{2p}} = \sigma_1(S_{M_1} - S_{m_1}) + \cdots + \sigma_p(S_{M_p} - S_{m_p}).$$

Using the fact that $X_1, X_2, \ldots$ are i.i.d. random variables, we obtain

$$\Sigma(B) = \sum_{\substack{m_1,\ldots,m_p \\ M_1,\ldots,M_p}} \varphi(\sigma_1 2\pi\alpha)^{M_1 - m_1} \cdots \varphi(\sigma_p 2\pi\alpha)^{M_p - m_p}, \quad (2.6)$$

where the summation is over all $m_1, \ldots, m_p$ and $M_1, \ldots, M_p$ satisfying (2.5), with the extra conditions that $m_k < M_k$ if $\sigma_k \neq 0$, and $m_k = M_k$ if $\sigma_k = 0$, for all $1 \leq k \leq p$.

Fix $M_1, \ldots, M_p$. Then (2.6) factors into p factors, the kth factor being a sum over m_k. If $\sigma_k \neq 0$, then the kth factor is

$$\sum_{M_{k-1} < m_k < M_k} \varphi(\sigma_k 2\pi\alpha)^{M_k - m_k} = \frac{\varphi(\sigma_k 2\pi\alpha)}{1 - \varphi(\sigma_k 2\pi\alpha)} - \frac{\varphi(\sigma_k 2\pi\alpha)^{M_k - M_{k-1}}}{1 - \varphi(\sigma_k 2\pi\alpha)},$$

where we use the convention that $M_0 = m$. If $\sigma_k = 0$, then the extra condition $m_k = M_k$ shows that the kth factor is simply 1. Let $A(\sigma_k) = \frac{\varphi(\sigma_k 2\pi\alpha)}{1 - \varphi(\sigma_k 2\pi\alpha)}$ if $\sigma_k \neq 0$, and $A(\sigma_k) = 1$ if $\sigma_k = 0$. Let, moreover

$$E(\sigma_k) = E(\sigma_k, M_{k-1}, M_k) = -\frac{\varphi(\sigma_k 2\pi\alpha)^{M_k - M_{k-1}}}{1 - \varphi(\sigma_k 2\pi\alpha)}$$

if $\sigma_k \neq 0$, and $E(\sigma_k) = 0$ if $\sigma_k = 0$. With this notation we thus have

$$\Sigma(B) = \sum_{m+1 \le M_1 < \cdots < M_p \le m+n} \prod_{k=1}^{p} \left(A(\sigma_k) + E(\sigma_k)\right). \tag{2.7}$$

Let us now expand the product in (2.7). The main term will come from $\prod_{k=1}^{p} A(\sigma_k)$. Indeed, all other terms are of the form $\prod_{k=1}^{p} a_k$, where a_k is either $A(\sigma_k)$ or $E(\sigma_k)$ for all $1 \le k \le p$, and $a_k = E(\sigma_k)$ for at least one k. Let k^* denote the largest index k such that $a_k = E(\sigma_k)$. If $\sigma_{k^*} = 0$, then $E(\sigma_{k^*}) = 0$ and so $\prod_{k=1}^{p} a_k = 0$. Else, by summing over M_{k^*} first, we can use the estimate

$$\left| \sum_{M_{k^*-1} < M_{k^*} < M_{k^*+1}} \frac{\varphi(\sigma_{k^*} 2\pi\alpha)^{M_{k^*} - M_{k^*-1}}}{1 - \varphi(\sigma_{k^*} 2\pi\alpha)} \right| \le \frac{2}{|1 - \varphi(\sigma_{k^*} 2\pi\alpha)|^2},$$

where $M_{p+1} = m + n + 1$ by convention in the case $k^* = p$. Applying Proposition 2.1, the subadditivity of $\|\cdot\|$ and the definition of R we obtain

$$1 - |\varphi(\sigma_{k^*} 2\pi\alpha)| \ge \left(\mathbb{E}\,\|2\alpha(X_1 - X_2)\|\right)^2 \ge \frac{1}{4}\left(\mathbb{E}\,\|4\alpha(X_1 - X_2)\|\right)^2 = \frac{4}{R},$$

$$\frac{2}{|1 - \varphi(\sigma_{k^*} 2\pi\alpha)|^2} \le \frac{R^2}{8}.$$

We similarly get $|a_k| \le \frac{R}{4}$. Since there are $\binom{n}{p-1}$ ways to fix $M_1, \ldots, M_{k^*-1}, M_{k^*+1}, \ldots, M_p$, we have

$$\left| \sum_{m+1 \le M_1 < \cdots < M_p \le m+n} \prod_{k=1}^{p} a_k \right| \le \binom{n}{p-1} \frac{R^{p+1}}{2 \cdot 4^p}.$$

Note that the main term $\prod_{k=1}^{p} A(\sigma_k)$ does not depend on $M_1, \ldots M_p$, and that there are 2^p terms in the expansion. Therefore

$$\Sigma(B) = \binom{n}{p} \prod_{k=1}^{p} A(\sigma_k) \pm \frac{R^{p+1} n^{p-1}}{2 \cdot 2^p (p-1)!}. \tag{2.8}$$

Let us fix π_e, π_o as before, and sum (2.8) over $\sigma \in \{-1, 0, 1\}^p$ to get

$$\sum_{\sigma\in\{-1,0,1\}^p} \Sigma(B(\pi_e,\pi_o,\sigma)) = \binom{n}{p}\prod_{k=1}^{p}\sum_{\sigma_k=-1}^{1} A(\sigma_k) \pm \frac{3^p R^{p+1} n^{p-1}}{2\cdot 2^p (p-1)!}.$$

Here

$$\sum_{\sigma_k=-1}^{1} A(\sigma_k) = \frac{\bar\varphi(2\pi\alpha)}{1-\bar\varphi(2\pi\alpha)} + 1 + \frac{\varphi(2\pi\alpha)}{1-\varphi(2\pi\alpha)} = \frac{1-|\varphi(2\pi\alpha)|^2}{|1-\varphi(2\pi\alpha)|^2}.$$

Since nothing depends on π_e and π_o, summing over them simply introduces a new factor of $p!^2$. By checking that

$$\frac{3^p p!^2}{2\cdot 2^p (p-1)!} \le p^{p+1},$$

we thus get

$$\sum_{\substack{B\\ q=p}} \Sigma(B) = \left(\frac{1-|\varphi(2\pi\alpha)|^2}{|1-\varphi(2\pi\alpha)|^2}\right)^p p!^2 \binom{n}{p} \pm (pR)^{p+1} n^{p-1}. \tag{2.9}$$

Now we estimate $\Sigma(B)$ in the case $q < p$. Using the fact that $X_1, X_2, \ldots$ are i.i.d. random variables, and $k_1 < \cdots < k_s$, it is easy to see that

$$\mathbb{E} e^{2\pi i\alpha\left(\varepsilon_1 S_{k_1} + \cdots + \varepsilon_s S_{k_s}\right)} = \varphi(2c_1\pi\alpha)^{k_1}\varphi(2c_2\pi\alpha)^{k_2-k_1}\cdots\varphi(2c_s\pi\alpha)^{k_s-k_{s-1}},$$

where $c_j = \varepsilon_j + \cdots + \varepsilon_s$. Hence

$$\Sigma(B) = \sum_{m+1\le k_1<\cdots<k_s\le m+n} \varphi(2c_1\pi\alpha)^{k_1}\varphi(2c_2\pi\alpha)^{k_2-k_1}\cdots\varphi(2c_s\pi\alpha)^{k_s-k_{s-1}}. \tag{2.10}$$

Consider the set

$$A = \left\{ k\in\mathbb{Z} \ : \ \mathbb{E}\,\|2k\alpha(X_1-X_2)\| < \frac{1}{4}\mathbb{E}\,\|4\alpha(X_1-X_2)\| \right\}.$$

Note that A does not contain any two consecutive integers. Indeed, if $k, k+1 \in A$, then the subadditivity of $\|\cdot\|$ implies

$$\|4\alpha(X_1 - X_2)\| \le 2\,\|2k\alpha(X_1 - X_2)\| + 2\,\|2(k+1)\alpha(X_1 - X_2)\|\,.$$

Taking the expected value of both sides we would thus get

$$\mathbb{E}\,\|4\alpha(X_1 - X_2)\| < \left(2 \cdot \frac{1}{4} + 2 \cdot \frac{1}{4}\right) \mathbb{E}\,\|4\alpha(X_1 - X_2)\|\,,$$

contradiction. Clearly A is symmetric (i.e. $k \in A$ implies $-k \in A$), $0 \in A$ and $\pm 1, \pm 2 \notin A$. Let

$$\{j \in [s] \ : \ c_j \in A\} = \{j_1, j_2, \ldots, j_M\}$$

where $j_1 < j_2 < \cdots < j_M$. Note that $c_1 = \varepsilon_1 + \cdots + \varepsilon_s = 0 \in A$, therefore $j_1 = 1$. For any $1 \le r \le M-1$ let $I_r = [j_r, j_{r+1})$, and let $I_M = [j_M, s]$. By the definition of c_j we have

$$c_{j_r} - c_{j_{r+1}} = \sum_{j \in I_r} \varepsilon_j, \qquad c_{j_M} = \sum_{j \in I_M} \varepsilon_j. \tag{2.11}$$

We claim $M < p$. Consider the following two cases.

Case 1. Assume $c_{j_1} = c_{j_2} = \cdots = c_{j_M} = 0$. Then (2.11) shows that $I_1, I_2, \ldots, I_M$ is a partition of $[s]$ into M intervals such that $\sum_{j \in I_r} \varepsilon_j = 0$ for every r. By the definition of $q = q(B)$ this means $M \le q < p$.

Case 2. Assume $c_{j_1}, c_{j_2}, \ldots, c_{j_M}$ are not all zero. Recalling that $c_{j_1} = c_1 = 0$, (2.11) shows that there exists an r such that $\sum_{j \in I_r} \varepsilon_j = a$ for some nonzero $a \in A$. Note $|a| \ge 3$. From the definition (2.4) of ε_j we thus obtain

$$\left|\bigcup_{j \in I_r} B_j\right| \ge \left|\sum_{j \in I_r} \varepsilon_j\right| = |a| \ge 3 \tag{2.12}$$

for this particular r. For any other r' (2.11) shows that $\sum_{j \in I_{r'}} \varepsilon_j$ is the difference of two elements of A. Since A does not contain any two consecutive integers, this difference cannot be ± 1. From the definition (2.4) of ε_j it is thus easy to see that

$$\left|\bigcup_{j \in I_{r'}} B_j\right| \ge 2. \tag{2.13}$$

Summing (2.13) over $r' \ne r$ and adding (2.12), we get

$$2p = \sum_{j=1}^{s} |B_j| \geq 2M + 1,$$

hence $M < p$ in this case as well.

We have thus proved that $M < p$. Set $\Phi = 1 - \frac{1}{R}$. According to Proposition 2.1, for any $j \neq j_1, \ldots, j_M$ we have

$$|\varphi(2c_j\pi\alpha)| \leq 1 - \left(\mathbb{E}\,\|2c_j\alpha(X_1 - X_2)\|\right)^2.$$

Since $c_j \notin A$, we have

$$\left(\mathbb{E}\,\|2c_j\alpha(X_1 - X_2)\|\right)^2 \geq \frac{1}{16}\left(\mathbb{E}\,\|4\alpha(X_1 - X_2)\|\right)^2 = \frac{1}{R},$$

showing $|\varphi(2c_j\pi\alpha)| \leq \Phi$.

Let us now apply the triangle inequality to (2.10), and let us use the estimate $|\varphi(2c_j\pi\alpha)| \leq \Phi$ whenever $j \neq j_1, \ldots, j_M$, and the trivial estimate $|\varphi(2c_j\pi\alpha)| \leq 1$ for $j = j_1, \ldots, j_M$. We get

$$|\Sigma(B)| \leq \sum_{m+1 \leq k_1 < \cdots < k_s \leq m+n} 1 \cdot \Phi^{k_{j_2-1} - k_{j_1}} \cdot 1 \cdot \Phi^{k_{j_3-1} - k_{j_2}} \cdots 1 \cdot \Phi^{k_s - k_{j_M}}.$$

Fix $k_{j_1}, \ldots, k_{j_M}$ and the exponent

$$k = (k_{j_2-1} - k_{j_1}) + (k_{j_3-1} - k_{j_2}) + \cdots + (k_s - k_{j_M}) \tag{2.14}$$

of Φ. Then for all $j \neq j_1, \ldots, j_M$ the integer k_j belongs to the set

$$[k_{j_1} + 1, k_{j_1} + k] \cup [k_{j_2} + 1, k_{j_2} + k] \cup \cdots \cup [k_{j_M} + 1, k_{j_M} + k]$$

of cardinality at most Mk. Hence for fixed $k_{j_1}, \ldots, k_{j_M}$ the number of s-tuples $(k_1, \ldots, k_s)$ for which (2.14) holds is at most $\binom{Mk}{s-M} \leq \frac{(Mk)^{s-M}}{(s-M)!}$, and so we get

$$\begin{aligned} |\Sigma(B)| &\leq \sum_{m+1 \leq k_{j_1} < \cdots < k_{j_M} \leq m+n} \sum_{k=0}^{\infty} \frac{(Mk)^{s-M}}{(s-M)!}\Phi^k \\ &\leq \frac{n^M}{M!} \cdot \frac{M^{s-M}}{(s-M)!} \sum_{k=0}^{\infty} k^{s-M}\Phi^k. \end{aligned}$$

Here $0 \le \Phi < 1$, therefore we can use a well-known Taylor expansion to obtain the estimate

$$\sum_{k=0}^{\infty} k^{s-M}\Phi^k \le \sum_{k=0}^{\infty}(k+s-M)\cdots(k+2)(k+1)\Phi^k = \frac{(s-M)!}{(1-\Phi)^{s-M+1}}.$$

Since $R = (1-\Phi)^{-1}$, we get

$$|\Sigma(B)| \le R^s \frac{M^{s-M}n^M}{M!R^{M-1}}.$$

Here $s \le 2p$, and $0 < M < p$. The total number of ordered partitions B of $[2p]$ is at most $(2p)^{2p}$, hence

$$\sum_{\substack{B \\ q<p}} |\Sigma(B)| \le (2pR)^{2p} \max_{0<q<p} \frac{q^{2p-q}n^q}{q!R^{q-1}}. \tag{2.15}$$

Since

$$\mathbb{E}\left|\sum_{k=m+1}^{m+n} e^{2\pi i S_k \alpha}\right|^{2p} = \sum_{\substack{B \\ q=p}} \Sigma(B) + \sum_{\substack{B \\ q<p}} \Sigma(B),$$

combining (2.9) and (2.15) finishes the proof.

□

3 Proof of Theorem 1.1

We distinguish between two main cases. First, we will assume

$$\mathbb{P}\left(4\alpha(X_1 - X_2) \in \mathbb{Z}\right) < 1, \tag{3.1}$$

in which case the proof will rely on Proposition 2.2. Note that (3.1) implies that $\exp(2\pi i X_1 \alpha)$ is non-degenerate, and it also implies condition $\mathbb{P}(2\alpha X_1 \in \mathbb{Z}) < 1$ from (i). Thus we will need to prove that (3.1) implies (1.4). Next, we will assume that $\mathbb{P}\left(4\alpha(X_1 - X_2) \in \mathbb{Z}\right) = 1$ and that $\exp(2\pi i X_1 \alpha)$ is non-degenerate. In this case we will use the theory of φ-mixing Markov chains in the proof.

Let us thus assume that (3.1) holds. Put $T_{m,n} = \sum_{k=m+1}^{m+n} e^{2\pi i S_k \alpha}$, $T_n = T_{0,n}$. Let $1 \le p \le 3\log\log n$, and apply Proposition 2.2 on $T_{m,n}$. It is easy to see that the error term in Proposition 2.2 satisfies

$$(2pR)^{2p} \max_{0<q<p} \frac{q^{2p-q}n^q}{q!R^{q-1}} + (pR)^{p+1}n^{p-1} \ll n^{p-1+\varepsilon}$$

for any $\varepsilon > 0$, with an implied constant depending only on α, ε and the distribution of X_1. For the main term we have

$$\left(\frac{1-|\varphi(2\pi\alpha)|^2}{|1-\varphi(2\pi\alpha)|^2}\right)^p p!^2\binom{n}{p} \sim \left(\frac{1-|\varphi(2\pi\alpha)|^2}{|1-\varphi(2\pi\alpha)|^2}\right)^p p!n^p.$$

Indeed, we only need to check that the limit of the sequence

$$1\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\cdots\left(1-\frac{p-1}{n}\right)$$

is 1. Standard computation shows that this sequence can be approximated by $e^{-(1+2+\cdots+(p-1))/n}$, and hence by $e^{-p^2/n}$, which clearly has limit 1. We thus have

$$\begin{aligned} \mathbb{E}|T_{m,n}|^{2p} \sim & c^p p!n^p \quad \text{as } n\to\infty, \\ & \text{uniformly for } \ m\geq 0, 1\leq p\leq 3\log\log n \end{aligned} \tag{3.2}$$

with

$$c = \frac{1-|\varphi(2\pi\alpha)|^2}{|1-\varphi(2\pi\alpha)|^2}. \tag{3.3}$$

We now show that (1.4) holds. We break the argument into lemmas. We follow the method of [8].

Lemma 3.1. *We have for any* $0<\varepsilon<1$,

$$\mathbb{P}\{|T_{m,n}| \geq ((1+2\varepsilon)cn\log\log n)^{1/2}\} \ll \exp(-(1+\varepsilon)\log\log n),$$

where the constant implied by $\ll$ *depends on the sequence* $(X_k), \alpha$ *and* ε.

Proof. Clearly, multiplying the terms of $T_{m,n}$ by $c^{-1/2}$, (3.2), (1.4) and the conclusion of Lemma 3.1 will be satisfied with $c=1$ and thus without loss of generality we can assume $c=1$. Let

$$G_{m,n}(t) = \mathbb{P}\{|T_{m,n}| \geq (tn\log\log n)^{1/2}\}, \qquad t>0$$

and

$$Z_{m,n} = |T_{m,n}|^2/(n\log\log n). \tag{3.4}$$

Using Stirling's formula, we get from (3.2) for $m \geq 0$, $n \geq n_0$ and $1 \leq p \leq 3 \log\log n$ that

$$\sqrt{p}(p/e)^p(\log\log n)^{-p} \ll \mathbb{E}Z_{m,n}^p \ll \sqrt{p}(p/e)^p(\log\log n)^{-p}. \tag{3.5}$$

Here, an in the sequel, the constants implied by $\ll$, $\gg$ depend (at most) on $(X_k), \alpha$ and ε. Thus by the Markov inequality

$$G_{m,n}(t) = \mathbb{P}(Z_{m,n} \geq t) \leq t^{-p}\mathbb{E}Z_n^p \ll t^{-p}\sqrt{p}(p/e)^p(\log\log n)^{-p}.$$

If $t \geq 3$, we choose $p = [e \log\log n]$ to get

$$G_{m,n}(t) \ll t^{-p}(\log\log n)^{1/2} \ll t^{-2\log\log n}, \qquad t \geq 3. \tag{3.6}$$

For $0 < t < 3$ we choose $p = [t \log\log n]$ to get

$$G_{m,n}(t) \ll (\log\log n)^{1/2} \exp(-t \log\log n) \qquad 0 < t < 3, \tag{3.7}$$

and choosing $t = 1 + 2\varepsilon$, Lemma 3.1 is proved. □

Lemma 3.2. *We have for any* $0 < \varepsilon < 1$,

$$\mathbb{P}\{|T_{m,n}| \geq ((1-\varepsilon)cn \log\log n)^{1/2}\} \gg \exp(-(1-\varepsilon^2/8)\log\log n).$$

Proof. As before, we can assume $c = 1$. We set

$D_1 = \{1 - \varepsilon \leq Z_{m,n} \leq 1\},\ D_2 = \{0 \leq Z_{m,n} < 1 - \varepsilon\},\ D_3 = \{1 < Z_{m,n} \leq 3\}$, $D_4 = \{Z_{m,n} > 3\}$,

where $Z_{m,n}$ is defined by (3.4). Then by (3.5) we have for $m \geq 0$, $n \geq n_0$ and $1 \leq p \leq 3 \log\log n$,

$$\begin{aligned} G_{m,n}(1-\varepsilon) &= \mathbb{P}(Z_{m,n} \geq 1 - \varepsilon) \geq \mathbb{P}(D_1) \geq \int_{D_1} Z_{m,n}^p \, d\mathbb{P} \\ &\geq A\sqrt{p}(p/e)^p(\log\log n)^{-p} - (I_2 + I_3 + I_4) \end{aligned} \tag{3.8}$$

where A is a constant and

$$I_k = \int_{D_k} Z_{m,n}^p \, d\mathbb{P}, \qquad k = 2, 3, 4.$$

We choose $p = [(1-\varepsilon/2)\log\log n]$ and estimate I_2, I_3 and I_4 from above. First we get, using $G_{m,n}(t) = P(Z_{m,n} \geq t)$ and (3.7),

$$\begin{aligned} I_2 &\leq p \int_0^{1-\varepsilon} t^{p-1} G_{m,n}(t)dt \\ &\ll p(\log\log n)^{1/2} \int_0^{1-\varepsilon} t^{p-1}\exp(-t\log\log n)dt \\ &= p(\log\log n)^{-(p-1/2)} \int_0^{(1-\varepsilon)\log\log n} u^{p-1}e^{-u}du. \end{aligned}$$

Since $u^{p-1}e^{-u}$ reaches its maximum at $u = p-1$ which exceeds the upper limit of the last integral by the choice of p, we get

$$\begin{aligned} I_2 &\ll p(\log\log n)^{1/2}(1-\varepsilon)^p e^{-(1-\varepsilon)\log\log n} \\ &\ll (\log\log n)^{3/2}\cdot(1-\varepsilon)^{(1-\varepsilon/2)\log\log n}(\log n)^{-(1-\varepsilon)} \\ &= (\log\log n)^{3/2}(\log n)^{-\gamma}, \end{aligned}$$

where

$$\gamma = 1-\varepsilon-(1-\varepsilon/2)\log(1-\varepsilon).$$

Similarly as above, we get

$$I_3 \ll p(\log\log n)^{-(p-1/2)} \int_{\log\log n}^{3\log\log n} u^{p-1}e^{-u}du.$$

Now the maximum of the integrand is reached at a point which is smaller than the lower limit of the integral and we get

$$I_3 \ll (\log\log n)^{3/2}(\log n)^{-1}. \tag{3.9}$$

Finally, to estimate I_4 we proceed as with I_2, but instead of (3.7) we use (3.6) to get

$$\begin{aligned} I_4 &\ll p\int_3^\infty t^{p-1}G_{m,n}(t)dt \ll p\int_3^\infty t^{p-1}t^{-2\log\log n}dt \\ &\ll (\log\log n)e^{-\log\log n} = (\log\log n)(\log n)^{-1}. \end{aligned}$$

Now using $p = [(1-\varepsilon/2)\log\log n]$ we see that the first term in the second line of (3.8) is

$$A\sqrt{p}(p/e)^p(\log\log n)^{-p} \gg (p/e)^p\left(\frac{p}{1-\varepsilon/2}\right)^{-p} \gg (\log n)^{-\gamma'}$$

where

$$\gamma' = (1-\varepsilon/2) - (1-\varepsilon/2)\log(1-\varepsilon/2).$$

For $0 < \varepsilon < 1$ we have $\gamma' < \gamma$ and $\gamma' < 1 - \varepsilon^2/8$. Indeed, after some simplification the inequality $\gamma' < \gamma$ is equivalent to

$$\log\left(1 - \frac{\varepsilon/2}{1-\varepsilon/2}\right) < -\frac{\varepsilon/2}{1-\varepsilon/2},$$

which follows from the general inequality $\log(1-x) < -x$, valid for any $0 < x < 1$. To see $\gamma' < 1 - \varepsilon^2/8$, since their values are equal at $\varepsilon = 0$, it will be enough to check that their derivatives with respect to ε satisfy

$$\frac{1}{2}\log(1-\varepsilon/2) < -\varepsilon/4$$

for all $0 < \varepsilon < 1$. This again follows from $\log(1-x) < -x$. This implies that all of I_2, I_3 and I_4 are of smaller order of magnitude than the first term in the second line of (3.8). Thus we get

$$G_{m,n}(1-\varepsilon) \gg (\log n)^{-\gamma'} \gg (\log n)^{-(1-\varepsilon^2/8)}$$

and Lemma 3.2 is proved. □

Lemma 3.3. *Let $\mathcal{F}_n$ denote the σ-algebra generated by $S_j, 1 \le j \le q^n$ and let $0 < \varepsilon < 1$. Then there exists a number $q_0(\varepsilon)$ such that for any $n \ge 1$ and any integer $q \ge q_0(\varepsilon)$ we have*

$$\begin{aligned} &\mathbb{P}\left(|T_{q^n}| \ge ((1-\varepsilon)cq^n \log\log q^n)^{1/2} \,|\, \mathcal{F}_{n-1}\right) \\ &\gg \exp(-(1-\varepsilon^2/32)\log\log q^n) \end{aligned} \tag{3.10}$$

with the exception on a set in the probability space with measure $\ll n^{-100}$.

Proof. Choosing again $c = 1$, as we may, we first note that by (3.2) and the Markov inequality we have, choosing $p = [\log\log n]$,

$$\begin{aligned} &\mathbb{P}\left(|T_n| \ge B(n\log\log n)^{1/2}\right) \le \frac{\mathbb{E}\left|\sum_{k=1}^n e^{2\pi i\alpha S_k}\right|^{2p}}{B^{2p}(n\log\log n)^p} \\ &\ll \frac{p!n^p}{B^{2p}(n\log\log n)^p} \le \frac{p^p n^p}{B^{2p}(np)^p} = B^{-2p} \le e^{-100p} \\ &\ll e^{-100\log\log n} = (\log n)^{-100} \end{aligned} \tag{3.11}$$

provided we choose the constant B large enough. Call a point $\omega \in \Omega$ "good" or "bad" according as the inequality

$$|T_{q^{n-1}}(\omega)| \le B(q^{n-1}\log\log q^{n-1})^{1/2} \tag{3.12}$$

holds or not. By (3.11) the set of bad ω's has total measure (probability) $\ll n^{-100}$. Consider now a good $\omega \in \Omega$. Letting $S_k^* = S_k - S_{q^{n-1}} = \sum_{j=q^{n-1}+1}^{k} X_j$ for $k > q^{n-1}$, we have

$$\begin{aligned} T_{q^n} &= T_{q^{n-1}} + \sum_{k=q^{n-1}+1}^{q^n} e^{2\pi i\alpha S_k} = T_{q^{n-1}} + \sum_{k=q^{n-1}+1}^{q^n} e^{2\pi i\alpha(S_{q^{n-1}}+S_k^*)} \\ &= T_{q^{n-1}} + e^{2\pi i\alpha S_{q^{n-1}}} \sum_{k=q^{n-1}+1}^{q^n} e^{2\pi i\alpha S_k^*} =: T_{q^{n-1}} + e^{2\pi i\alpha S_{q^{n-1}}} T^*_{q^{n-1},q^n}. \end{aligned} \tag{3.13}$$

Here $T_{q^{n-1}}$ and $e^{2\pi i\alpha S_{q^{n-1}}}$ are $\mathcal{F}_{n-1}$ measurable and thus the conditional probability in (3.10) can be evaluated by using (3.13) and substituting the values of these variables at ω. Since ω is a good point, for $T_{q^{n-1}}$ we have the estimate (3.12), further $|e^{2\pi i\alpha S_{q^{n-1}}}| = 1$ and thus observing that $T^*_{q^{n-1},q^n}$ is independent of $\mathcal{F}_{n-1}$, we get

$$\begin{aligned} &\mathbb{P}\left(|T_{q^n}| \ge ((1-\varepsilon)q^n\log\log q^n)^{1/2} \,|\, \mathcal{F}_{n-1}\right) \\ &\ge \mathbb{P}\left(|T^*_{q^{n-1},q^n}| \ge ((1-\varepsilon)q^n\log\log q^n)^{1/2} + B(q^{n-1}\log\log q^{n-1})^{1/2}\Big|\, \mathcal{F}_{n-1}\right) \\ &= \mathbb{P}\left(|T^*_{q^{n-1},q^n}| \ge ((1-\varepsilon)q^n\log\log q^n)^{1/2} + B(q^{n-1}\log\log q^{n-1})^{1/2}\right) \\ &\ge \mathbb{P}\left(|T^*_{q^{n-1},q^n}| \ge ((1-\varepsilon/2)q^n\log\log q^n)^{1/2}\right) \\ &\gg \exp(-(1-\varepsilon^2/32)\log\log q^n) \end{aligned}$$

provided $q \ge q_0(\varepsilon)$, where in the last step we used Lemma 3.2 for the exponential sum $T^*_{q^{n-1},q^n}$ belonging to the i.i.d. sequence $\{X_j,\, j = q^{n-1}+1, q^{n-1}+2, \ldots\}$. This completes the proof of Lemma 3.3. □

The following is Lévy's conditional form of the Borel–Cantelli lemma; see e.g. [26], p. 124.

Lemma 3.4. *Let $A_1, A_2, \ldots$ be arbitrary events, let $\mathcal{F}_1 \subset \mathcal{F}_2, \ldots$ be σ-algebras such that A_n is $\mathcal{F}_n$ measurable and $\sum_{n=1}^{\infty} \mathbb{P}(A_n|\mathcal{F}_{n-1}) = +\infty$ a.s. Then with probability 1, infinitely many A_n occur.*

We are now in a position to prove (1.4). We first observe that Lemma 3.1 and the Borel–Cantelli lemma imply

$$\limsup_{n\to\infty} (c[\theta^n]\log\log[\theta^n])^{-1/2} T_{[\theta^n]} \le 1 \quad \text{a.s.} \tag{3.14}$$

for any real $\theta > 1$. On the other hand, (3.2) and the Erdős–Stechkin inequality (see [18], Theorem A) imply

$$\mathbb{E} \max_{1\le\ell\le[\theta^{n+1}]-[\theta^n]} |T_{[\theta^n],\ell}|^{2p} \le K c^p p!([\theta^{n+1}]-[\theta^n])^p$$

with some constant $K > 0$. Thus by the Markov inequality we get, choosing $p \sim \log\log[\theta^n] \sim \log n$

$$\begin{aligned}
&\mathbb{P}\left\{ \max_{1\le\ell\le[\theta^{n+1}]-[\theta^n]} |T_{[\theta^n],\ell}| \ge A(c([\theta^{n+1}]-[\theta^n])\log\log([\theta^{n+1}]-[\theta^n]))^{1/2} \right\} \\
&\ll \frac{K c^p p!([\theta^{n+1}]-[\theta^n])^p}{A^{2p} c^p ([\theta^{n+1}]-[\theta^n])^p (\log\log([\theta^{n+1}]-[\theta^n]))^p} \ll \frac{K p^p}{A^{2p}(\log n)^p} \\
&\ll K(2A^{-2})^p \ll n^{-2}
\end{aligned}$$

provided A is large enough. Choosing θ sufficiently close to 1, we have $[\theta^{n+1}] - [\theta^n] \le \varepsilon^2[\theta^n]$ for $n \ge n_0(\varepsilon)$ and thus the previous probability bound and the Borel–Cantelli lemma imply

$$\max_{1\le\ell\le[\theta^{n+1}]-[\theta^n]} |T_{[\theta^n],\ell}| \ll \varepsilon([\theta^n]\log\log[\theta^n])^{1/2} \quad \text{a.s.}$$

The last relation and (3.14) together imply the $\le$ inequality in (1.4). To prove the $\ge$ inequality, fix $0 < \varepsilon < 1$ and let $q \ge q_0(\varepsilon)$ be an integer, where $q_0(\varepsilon)$ is the threshold number in Lemma 3.3. Put

$$A_n = \left\{ |T_{q^n}| \ge ((1-\varepsilon)cq^n \log\log q^n)^{1/2} \right\}$$

and let $\mathcal{F}_n = \sigma\{S_1, \dots S_{q^n}\}$. Then Lemma 3.3 shows that for any $n \ge 1$ the inequality

$$\mathbb{P}(A_n|\mathcal{F}_{n-1}) \gg \exp(-(1-\varepsilon^2/32)\log\log q^n) \tag{3.15}$$

holds with probability $\ge 1 - Cn^{-100}$ for some constant C. By the (ordinary) Borel–Cantelli lemma this implies that with probability 1 the inequality (3.15) holds for sufficiently large n and thus $\mathbb{P}(A_n|\mathcal{F}_{n-1}) = +\infty$ a.s. Thus the inequality $\ge$ in (1.4) follows from Lemma 3.4, completing the proof of Theorem 1.1 in the case when (3.1) holds.

Next we assume

$$\mathbb{P}(4\alpha(X_1 - X_2) \in \mathbb{Z}) = 1, \tag{3.16}$$

and that $\exp(2\pi i X_1 \alpha)$ is non-degenerate. Recall that a sequence $(\boldsymbol{\xi}_k)$ of $\mathbb{C}$- or $\mathbb{R}^d$-valued random variables is called φ-mixing with mixing rate $\varphi(n)$ if

$$\varphi(n) := \sup_k \sup_{A \in \mathcal{F}_{1,k}, B \in \mathcal{F}_{k+n,\infty}} |\mathbb{P}(A|B) - \mathbb{P}(A)| \to 0$$

as $n \to \infty$, where $\mathcal{F}_{a,b}$ denotes the σ-algebra generated by the random variables $\{\boldsymbol{\xi}_j : a \leq j \leq b\}$. We claim that $(\exp(2\pi i S_k \alpha))$ is φ-mixing with exponential rate $\varphi(n) = O(e^{-\lambda n})$ for some positive constant λ.

We first note that (3.16) implies that there exists a constant $a \in \mathbb{R}$ such that

$$\mathbb{P}\left(e^{2\pi i X_1 \alpha} \in \left\{\pm e^{2\pi i a}, \pm i e^{2\pi i a}\right\}\right) = 1. \tag{3.17}$$

Without loss of generality we may assume that

$$\mathbb{P}\left(e^{2\pi i X_1 \alpha} = e^{2\pi i a}\right) > 0. \tag{3.18}$$

Let $\boldsymbol{\xi}_k = \exp(2\pi i(S_k \alpha - ka))$.

First, suppose that

$$\mathbb{P}\left(e^{2\pi i X_1 \alpha} \in \left\{\pm i e^{2\pi i a}\right\}\right) > 0. \tag{3.19}$$

Using (3.17), we get that $\boldsymbol{\xi}_k \in \{\pm 1, \pm i\}$. Since $X_1, X_2, \ldots$ are i.i.d., the sequence $(\boldsymbol{\xi}_k)$ is in fact a Markov chain with state space $\{\pm 1, \pm i\}$. The assumption (3.19) implies that it is possible to get from any state to any other state, i.e. that this Markov chain is irreducible. From (3.18) we can see that $\mathbb{P}(\boldsymbol{\xi}_{k+1} = \boldsymbol{\xi}_k) > 0$. This clearly implies that given any state, the greatest common divisor of the possible number of steps to return to the same state is 1, i.e. that this Markov chain is aperiodic. By a basic result for Markov chains (see e.g. Lemma 3 in [19]), p. 209), $(\boldsymbol{\xi}_k)$ is geometrically ergodic and thus φ-mixing with exponential rate. Replacing $\boldsymbol{\xi}_k$ by $\exp(2\pi i S_k \alpha) = e^{2\pi i k a} \boldsymbol{\xi}_k$, the finite state space property of $(\boldsymbol{\xi}_k)$ can be destroyed, but the dependence properties of $(\boldsymbol{\xi}_k)$ do not change and thus $\exp(2\pi i S_k \alpha)$ is also φ-mixing with exponential rate.

Suppose now that

$$\mathbb{P}\left(e^{2\pi i X_1 \alpha} \in \left\{\pm i e^{2\pi i a}\right\}\right) = 0.$$

This, together with (3.17), shows that in fact

$$\mathbb{P}\left(e^{2\pi i X_1 \alpha} \in \left\{\pm e^{2\pi i a}\right\}\right) = 1.$$

Therefore we now have $\boldsymbol{\xi}_k \in \{\pm 1\}$. Since $X_1, X_2, \ldots$ are i.i.d., the sequence $(\boldsymbol{\xi}_k)$ is again a Markov chain, this time with state space $\{\pm 1\}$. Since $\exp(2\pi i X_1 \alpha)$ is non-degenerate, we have

$$\mathbb{P}\left(e^{2\pi i X_1 \alpha} = e^{2\pi i a}\right) > 0, \qquad \mathbb{P}\left(e^{2\pi i X_1 \alpha} = -e^{2\pi i a}\right) > 0,$$

i.e. $\mathbb{P}(\boldsymbol{\xi}_{k+1} = \boldsymbol{\xi}_k) > 0$ and $\mathbb{P}(\boldsymbol{\xi}_{k+1} = -\boldsymbol{\xi}_k) > 0$. Hence the Markov chain $(\boldsymbol{\xi}_k)$ is also irreducible and aperiodic, and therefore φ-mixing with exponential rate. As before, $\exp(2\pi i S_k \alpha)$ is also φ-mixing with exponential rate.

We have thus proved that $(\exp(2\pi i S_k \alpha))$ is φ-mixing with exponential rate. We are going to use the following law of the iterated logarithm for weakly dependent random vectors.

Lemma 3.5. *Let $\boldsymbol{\xi}_1, \boldsymbol{\xi}_2, \ldots$ be a sequence of uniformly bounded random vectors in $\mathbb{R}^d$, $d \geq 1$ satisfying $\mathbb{E}\boldsymbol{\xi}_k = 0$ for all $k \geq 1$, and assume that the sequence $(\boldsymbol{\xi}_k)$ is φ-mixing with exponential rate. Assume that for some matrix Σ we have*

$$\lim_{n\to\infty} \frac{1}{n} Cov\left(\boldsymbol{\xi}_{m+1} + \ldots + \boldsymbol{\xi}_{m+n}\right) = \Sigma \tag{3.20}$$

for any $m \geq 0$, uniformly in m, where $Cov(\boldsymbol{\xi})$ denotes the covariance matrix of a vector $\boldsymbol{\xi}$. Then with probability 1 the set of accumulation points of

$$\left\{ \frac{1}{(2n \log\log n)^{1/2}} \sum_{k=1}^{n} \boldsymbol{\xi}_k, \quad n = 1, 2, \ldots \right\}$$

is the unit ball K of the reproducing kernel Hilbert space defined by the matrix Σ. In particular, if Σ is diagonal with diagonal elements $\sigma_j^2, 1 \leq j \leq d$, then K is the ellipsoid $\{(x_1, \ldots, x_d) : \sum_{j=1}^{d} x_j^2/\sigma_j^2 \leq 1\}$.

Proof. Split $\mathbb{N}$ into consecutive blocks $I_1, J_1, I_2, J_2, \ldots$ such that the cardinality of I_k is $[k^{1/2}]$ and the cardinality of J_k is $[k^{1/4}]$. Put

$$\mathbf{U}_k = \sum_{j \in I_k} \boldsymbol{\xi}_j, \qquad \mathbf{V}_k = \sum_{j \in J_k} \boldsymbol{\xi}_j.$$

Since the gap between I_k and I_{k+1} is $[k^{1/4}]$ and $(\boldsymbol{\xi}_k)$ is φ-mixing with exponential rate, by Theorem 2 of [5] there exist independent random vectors $\mathbf{U}_k^*$, $k = 1, 2, \ldots$ such that $\mathbf{U}_k^*$ has the same distribution as $\mathbf{U}_k$ and

$$\mathbb{P}(|\mathbf{U}_k - \mathbf{U}_k^*| \geq Ce^{-\lambda k^{1/4}}) \leq Ce^{-\lambda k^{1/4}}, \quad k = 1, 2, \ldots \tag{3.21}$$

for some positive constants C, λ. Thus by the Borel–Cantelli lemma

$$|\mathbf{U}_k - \mathbf{U}_k^*| = O(e^{-\lambda k^{1/4}}) \qquad \text{a.s.} \tag{3.22}$$

Also, (3.21) and the uniform boundedness of $(\boldsymbol{\xi}_k)$ imply $\mathbb{E}|\mathbf{U}_k - \mathbf{U}_k^*| = O(\sqrt{k}e^{-\lambda k^{1/4}})$ and thus by $\mathbb{E}\mathbf{U}_k = 0$ we have $|\mathbb{E}\mathbf{U}_k^*| = O(\sqrt{k}e^{-\lambda k^{1/4}})$. Replacing $\mathbf{U}_k^*$ with $\mathbf{U}_k^* - \mathbb{E}\mathbf{U}_k^*$ we will have $\mathbb{E}\mathbf{U}_k^* = 0$, moreover (3.21) and (3.22) remain valid with a possibly smaller value of λ. Put $\mathrm{Cov}\,(\mathbf{U}_k) = \Sigma_k$, $\mathrm{Cov}\,(\mathbf{U}_k^*) = \Sigma_k^*$. Then $|\Sigma_k - \Sigma_k^*| = O(e^{-\lambda' k^{1/4}})$ entrywise; also by the assumption (3.20) we have

$$\Sigma_k \sim [k^{1/2}]\Sigma, \quad \Sigma_k^* \sim [k^{1/2}]\Sigma \quad \text{as } k \to \infty \tag{3.23}$$

uniformly in all entries of Σ_k and Σ_k^*, where Σ is the limit matrix in (3.20). It follows then that

$$\frac{1}{k^{3/2}}(\Sigma_1^* + \ldots + \Sigma_k^*) \to \Sigma \qquad \text{as } k \to \infty. \tag{3.24}$$

Since $|\mathbf{U}_k| = O(\sqrt{k})$ and $\mathbf{U}_k^*$ has the same distribution as $\mathbf{U}_k$, we have $|\mathbf{U}_k^*| = O(\sqrt{k})$ and thus applying Theorem 1 of Berning [7] with $s_n = n^{3/4}$ it follows that with probability 1 the set of accumulation points of

$$\left\{ (2n^{3/2} \log\log n)^{-1/2} \sum_{k=1}^{n} \mathbf{U}_k^*, \quad n \geq 1 \right\}$$

is the unit ball K of the reproducing kernel Hilbert space determined by the matrix Σ. By (3.22) the same holds if $\mathbf{U}_k^*$ is replaced with $\mathbf{U}_k$. Repeating the argument for the short block sums $\mathbf{V}_k$, $\mathbf{V}_k^*$, we get that with probability 1 the set of accumulation points of

$$\left\{ (2n^{5/4} \log\log n)^{-1/2} \sum_{k=1}^{n} \mathbf{V}_k^*, \quad n \geq 1 \right\}$$

is K and thus

$$\lim_{n\to\infty} (2n^{3/2} \log\log n)^{-1/2} \sum_{k=1}^{n} \mathbf{V}_k^* = 0 \qquad \text{a.s.}$$

We thus see that almost surely the set of accumulation points of

$$\left\{(2n^{3/2}\log\log n)^{-1/2}\sum_{k=1}^{n}(\mathbf{U}_k^*+\mathbf{V}_k^*),\quad n\geq 1\right\}$$

and its analogue for $\mathbf{U}_k+\mathbf{V}_k$ is K, proving Lemma 3.5 along the indices $n=N_k$, where $N_k=\sum_{j=1}^{k}[j^{1/2}]$. By the uniform boundedness of the $\boldsymbol{\xi}_k$, the maximal fluctuation of $\sum_{j=1}^{n}\boldsymbol{\xi}_j$ for $N_k\leq n\leq N_{k+1}$ is $O(N_{k+1}-N_k)=O(k^{1/2})$ and thus Lemma 3.5 holds for all indices n. □

Set

$$Y_k=\cos(2\pi S_k\alpha),\quad Z_k=\sin(2\pi S_k\alpha).$$

For any $1\leq k\leq\ell$ the random variables S_k and $S_\ell-S_k$ are independent, hence

$$\mathbb{E}\cos(2\pi S_k\alpha)\cos(2\pi S_\ell\alpha)=\frac{1}{2}\mathbb{E}\cos(2\pi(S_\ell-S_k)\alpha)+\frac{1}{2}\mathbb{E}\cos(2\pi(S_\ell+S_k)\alpha)$$
$$=\frac{1}{2}\mathrm{Re}\left[\mathbb{E}(e^{2\pi i(S_\ell-S_k)\alpha})+\mathbb{E}(e^{2\pi i(S_\ell+S_k)\alpha})\right]=\frac{1}{2}\mathrm{Re}\big[\mathbb{E}(e^{2\pi i(S_\ell-S_k)\alpha})$$
$$+\mathbb{E}(e^{2\pi i(S_\ell-S_k)\alpha})\mathbb{E}(e^{4\pi i S_k\alpha})\big]=\frac{1}{2}\mathrm{Re}\left(\varphi(2\pi\alpha)^{\ell-k}+\varphi(2\pi\alpha)^{\ell-k}\varphi(4\pi\alpha)^k\right)$$

and thus

$$\mathbb{E}Y_kY_\ell=\frac{1}{2}\mathrm{Re}\left(\varphi(2\pi\alpha)^{\ell-k}+\varphi(2\pi\alpha)^{\ell-k}\varphi(4\pi\alpha)^k\right).$$

Therefore

$$\mathbb{E}\left(\sum_{k=m+1}^{m+n}Y_k\right)^2=\mathrm{Re}\sum_{m+1\leq k<\ell\leq m+n}\left(\varphi(2\pi\alpha)^{\ell-k}+\varphi(2\pi\alpha)^{\ell-k}\varphi(4\pi\alpha)^k\right)$$
$$+\frac{1}{2}\mathrm{Re}\left(n+\sum_{k=m+1}^{m+n}\varphi(4\pi\alpha)^k\right)\tag{3.25}$$

and similarly

$$\mathbb{E}\left(\sum_{k=m+1}^{m+n}Z_k\right)^2=\mathrm{Re}\sum_{m+1\leq k<\ell\leq m+n}\left(\varphi(2\pi\alpha)^{\ell-k}-\varphi(2\pi\alpha)^{\ell-k}\varphi(4\pi\alpha)^k\right)$$
$$+\frac{1}{2}\mathrm{Re}\left(n-\sum_{k=m+1}^{m+n}\varphi(4\pi\alpha)^k\right)\tag{3.26}$$

and

$$\mathbb{E}\left(\sum_{k=m+1}^{m+n} Y_k\right)\left(\sum_{k=m+1}^{m+n} Z_k\right) = \mathrm{Im}\left(\sum_{m+1\le k<\ell\le m+n} \varphi(2\pi\alpha)^{\ell-k}\varphi(4\pi\alpha)^k\right)$$
$$+\frac{1}{2}\mathrm{Im}\left(n-\sum_{k=m+1}^{m+n}\varphi(4\pi\alpha)^k\right). \tag{3.27}$$

Now we prove (i). Assume that $\exp(2\pi i X_1\alpha)$ is non-degenerate, that $\mathbb{P}\left(2X_1\alpha\in\mathbb{Z}\right)<1$ and that (3.16) holds. The first two conditions imply that $|\varphi(2\pi\alpha)|<1$ and that $\varphi(4\pi\alpha)\neq 1$. We claim that

$$\sum_{m+1\le k<\ell\le m+n}\varphi^{\ell-k}(2\pi\alpha)\varphi^k(4\pi\alpha)=O(1)\quad\text{uniformly in } m. \tag{3.28}$$

Indeed, if $\varphi(4\pi\alpha)\neq\varphi(2\pi\alpha)$, then by fixing the index k first, we get that the sum in (3.28) is

$$\sum_{m+1\le k<m+n}\varphi(4\pi\alpha)^k\varphi(2\pi\alpha)\frac{\varphi(2\pi\alpha)^{m+n-k}-1}{\varphi(2\pi\alpha)-1}.$$

Here we have a partial sum of two geometric series with quotients $\varphi(4\pi\alpha)\neq 1$ and $\frac{\varphi(2\pi\alpha)}{\varphi(4\pi\alpha)}\neq 1$, therefore it is easy to see that

$$\sum_{m+1\le k<\ell\le m+n}\varphi^{\ell-k}(2\pi\alpha)\varphi^k(4\pi\alpha)=O(1)\quad\text{uniformly in } m.$$

If, on the other hand $\varphi(4\pi\alpha)=\varphi(2\pi\alpha)$, then the sum in (3.28) is

$$\sum_{m+1<\ell\le m+n}(\ell-m-1)\varphi(2\pi\alpha)^\ell=\varphi(2\pi\alpha)^{m+2}\sum_{r=1}^{n-1}r\varphi(2\pi\alpha)^{r-1}.$$

Here $|\varphi(2\pi\alpha)|^{m+2}<1$, and the sum is also $O(1)$, because it is a partial sum of a convergent series. Since we clearly also have

$$\sum_{k=m+1}^{m+n}\varphi(4\pi\alpha)^k=O(1)\quad\text{uniformly in } m,$$

formulas (3.25)–(3.27) simplify to

$$\mathbb{E}\left(\sum_{k=m+1}^{m+n} Y_k\right)^2 = \mathbb{E}\left(\sum_{k=m+1}^{m+n} Z_k\right)^2 =$$

$$\operatorname{Re}\sum_{m+1\le k<\ell\le m+n} \varphi(2\pi\alpha)^{\ell-k} + \frac{n}{2} + O(1),$$

$$\mathbb{E}\left(\sum_{k=m+1}^{m+n} Y_k\right)\left(\sum_{k=m+1}^{m+n} Z_k\right) = O(1),$$

both uniformly in m. Here we have

$$\sum_{m+1\le k<\ell\le m+n} \varphi(2\pi\alpha)^{\ell-k} = \sum_{r=1}^{n-1}(n-r)\varphi(2\pi\alpha)^r = n\sum_{r=1}^{n-1}\varphi(2\pi\alpha)^r + O(1) =$$

$$n\frac{\varphi(2\pi\alpha)}{1-\varphi(2\pi\alpha)} + O(1) \quad \text{uniformly in } m,$$

therefore

$$\lim_{n\to\infty}\frac{1}{n}\mathbb{E}\left(\sum_{k=m+1}^{m+n} Y_k\right)^2 = \lim_{n\to\infty}\frac{1}{n}\mathbb{E}\left(\sum_{k=m+1}^{m+n} Z_k\right)^2 =$$

$$\frac{1}{2} + \operatorname{Re}\frac{\varphi(2\pi\alpha)}{1-\varphi(2\pi\alpha)} = \frac{1-|\varphi(2\pi\alpha)|^2}{2|1-\varphi(2\pi\alpha)|^2} \tag{3.29}$$

and

$$\lim_{n\to\infty}\frac{1}{n}\mathbb{E}\left(\sum_{k=m+1}^{m+n} Y_k\right)\left(\sum_{k=m+1}^{m+n} Z_k\right) = 0 \tag{3.30}$$

uniformly in m.

Let now $Y_k^* = Y_k - \mathbb{E}Y_k$, $Z_k^* = Z_k - \mathbb{E}Z_k$. Clearly $\mathbb{E}Y_k = \operatorname{Re}\varphi(2\pi\alpha)^k$, $\mathbb{E}Z_k = \operatorname{Im}\varphi(2\pi\alpha)^k$, and since $|\varphi(2\pi\alpha)| < 1$, there exists a $0 < \rho < 1$ such that $|\mathbb{E}Y_k| \le \rho^k$, $|\mathbb{E}Z_k| \le \rho^k$. From this it follows that (3.29) and (3.30) remain valid if we replace Y_k and Z_k by Y_k^* and Z_k^*, respectively, and thus letting

$$\boldsymbol{\xi}_k = (Y_k, Z_k), \quad \boldsymbol{\xi}_k^* = (Y_k^*, Z_k^*)$$

it follows that the sequence $(\boldsymbol{\xi}_k^*)$ satisfies the assumptions of Lemma 3.5 in dimension $d = 2$ with a diagonal matrix Σ. Thus by Lemma 3.5 the set of accumulation points of

$$\left\{ \frac{1}{(2n \log\log n)^{1/2}} \sum_{k=1}^{n} \boldsymbol{\xi}_k^*,\ n = 1, 2, \dots \right\}$$

is, with probability 1, the circle around the origin with radius

$$\frac{\sqrt{1 - |\varphi(2\pi\alpha)|^2}}{\sqrt{2}|1 - \varphi(2\pi\alpha)|}.$$

By the exponential decrease of $\mathbb{E}|\boldsymbol{\xi}_k|$, the same holds if $\boldsymbol{\xi}_k^*$ is replaced by $\boldsymbol{\xi}_k$ and thus (1.4) is proved.

Finally, we prove (ii). Assume that $\exp(2\pi i X_1 \alpha)$ is non-degenerate and that $\mathbb{P}(2X_1\alpha \in \mathbb{Z}) = 1$. Note that the latter condition in fact implies (3.16). In this case

$$Z_k = \sin(2\pi S_k \alpha) = 0 \quad \text{a.s.}$$

which means that $\exp(2\pi i S_k \alpha) = Y_k \in \mathbb{R}$. We also have $\varphi(4\pi\alpha) = 1$. Thus (3.25) simplifies to

$$\mathbb{E}\left(\sum_{k=m+1}^{m+n} Y_k \right)^2 = 2\mathrm{Re} \sum_{m+1 \le k < \ell \le m+n} \varphi(2\pi\alpha)^{\ell-k} + 2n.$$

As before, we have

$$\sum_{m+1 \le k < \ell \le m+n} \varphi(2\pi\alpha)^{\ell-k} = \sum_{r=1}^{n-1} (n-r)\varphi(2\pi\alpha)^r = n \sum_{r=1}^{n-1} \varphi(2\pi\alpha)^r + O(1) =$$

$$n \frac{\varphi(2\pi\alpha)}{1 - \varphi(2\pi\alpha)} + O(1) \quad \text{uniformly in } m,$$

therefore

$$\lim_{n\to\infty} \frac{1}{n} \mathbb{E}\left(\sum_{k=m+1}^{m+n} Y_k \right)^2 = \frac{1 - |\varphi(2\pi\alpha)|^2}{|1 - \varphi(2\pi\alpha)|^2} \tag{3.31}$$

uniformly in m.

Let now $Y_k^* = Y_k - \mathbb{E}Y_k$. Clearly $\mathbb{E}Y_k = \operatorname{Re}\varphi(2\pi\alpha)^k$, and since $|\varphi(2\pi\alpha)| < 1$, there exists a $0 < \rho < 1$ such that $|\mathbb{E}Y_k| \le \rho^k$. From this it follows that (3.31) remains valid if we replace Y_k by Y_k^*, and thus it follows that the sequence (Y_k^*) satisfies the assumptions of Lemma 3.5 in dimension $d = 1$. Thus by Lemma 3.5 the set of accumulation points of

$$\left\{ \frac{1}{(2n\log\log n)^{1/2}} \sum_{k=1}^{n} Y_k^*,\ n = 1, 2, \dots \right\}$$

is, with probability 1, the closed interval centered at zero with radius

$$\frac{\sqrt{1 - |\varphi(2\pi\alpha)|^2}}{|1 - \varphi(2\pi\alpha)|}.$$

By the exponential decrease of $\mathbb{E}|Y_k|$, the same holds if Y_k^* is replaced by Y_k and thus (1.5) is proved.

□

In conclusion we prove, using a standard argument in uniform distribution theory (see e.g. [16], pp. 124–125) the remark made at the end of the Introduction concerning the discrepancy of $\{S_k\alpha\}$. Assume that X_1 is integer valued, it has mean zero and finite variance and (1.8) holds for infinitely many rationals p/q with some $C > 0$, $\gamma > 2$. Take such a rational p/q, fix $\varepsilon > 0$ and set $N = [q^\beta]$, where $\beta = (\gamma - 1)/(1/2 + \varepsilon)$. By the law of the iterated logarithm we have $|S_n| = O(n^{(1+\varepsilon)/2})$ a.s., pick a point ω in the probability space for which this holds. Then $\alpha = p/q + C\theta/q^\gamma$ with $|\theta| \le 1$ and thus for $1 \le n \le N$ we have $S_n\alpha = S_n p/q + \theta_n$ with

$$|\theta_n| \le C' N^{(1+\varepsilon)/2} q^{-\gamma} < C' q^{\beta(1+\varepsilon)/2-\gamma} = C' q^{-1-\delta}$$

where $\delta = \gamma - 1 - \beta(1+\varepsilon)/2 > 0$. Since S_n is an integer, none of the numbers

$$\{S_1\alpha\}, \{S_2\alpha\}, \dots, \{S_N\alpha\} \tag{3.32}$$

lie in the interval $[C'q^{-1-\delta}, 1/q - C'q^{-1-\delta}]$ and thus the discrepancy of the sequence (3.32) is $\ge 1/(2q)$. Since the choice of N implies $q \le (2N)^{1/\beta}$, if follows that, given any $\varepsilon > 0$, the discrepancy of the sequence (3.32) exceeds $C''N^{-1/\beta} = C''N^{-(1/2+\varepsilon)/(\gamma-1)}$. Since ε can be chosen to be arbitrarily small, our claim is proved.

References

[1] Aistleitner, C. and Fukuyama, K.: On the law of the iterated logarithm for trigonometric series with bounded gaps. Prob. Theory Related Fields 154 (2012), 607-620.

[2] Aistleitner, C. and Fukuyama, K.: On the law of the iterated logarithm for trigonometric series with bounded gaps II. J. Théor. Nombres Bordeaux 28 (2016), 391–416.

[3] Berkes, I.: A central limit theorem for trigonometric series with small gaps. Z. Wahrscheinlichkeitstheorie verw. Geb. 47 (1979), 157–161.

[4] Berkes, I.: An optimal condition for the LIL for trigonometric series. Trans. Amer. Math. Soc. 347 (1995) 515–530.

[5] Berkes, I. and Philipp, W.: Approximation theorems for independent and weakly dependent random vectors. Ann. of Probability 7 (1979) 29–54.

[6] Berkes, I. and Weber, M.: On the convergence of $\sum c_k f(n_k x)$. Memoirs of the AMS 201 (2009), no. 943, viii+72.

[7] Berning, J.: On the multivariate law of the iterated logarithm. Ann. of Probability 7 (1979), 980–988.

[8] Erdős, P. and Gál, I.: On the law of the iterated logarithm. Proc. Konink. Nederl. Akad. Wetensch. 58 (1955), 65–76.

[9] Feller, W.: An Introduction to Probability Theory and its Applications, Vol. II. Wiley, 1971,

[10] Fiedler, H., Jurkat, W. and Körner, O.: Asymptotic expansion of finite theta series. Acta Arithmetica 32 (1977), 129–146.

[11] Fukuyama, K.: A central limit theorem and a metric discrepancy result for sequences with bounded gaps. Dependence in probability, analysis and number theory, 233–246, Kendrick Press, Heber City, 2010.

[12] Fukuyama, K.: On the law of the iterated logarithm for trigonometric series with bounded gaps. Probab. Theory Related Fields 154 (2012), 607–620.

[13] Halberstam, H. and Roth, K.: Sequences. Oxford University Press 1966.

[14] Hardy, G. H. and Littlewood, J. E.: The trigonometric series associated with the elliptic ϑ-functions. Acta Math. 37 (1914), 193–238.

[15] Kaufman, R.: On the approximation of lacunary series with Brownian motion. Acta Math. Acad. Sci. Hung. 35 (1980), 61–66.

[16] Kuipers, L. and Niederreiter, H.: Uniform Distribution of Sequences. Wiley, 1974.

[17] Lévy, P.: Sur les series dont les termes sont des variables eventuelles independantes. Studia Math. 3 (1931), 119–155.

[18] Móricz, F.: Moment inequalities and the strong laws of large numbers. Z. Wahrscheinlichkeitstheorie und Verw. Gebiete 35 (1976), 299–314.

[19] Rosenblatt, M.: Markov Processes. Structure and Asymptotic Behavior. Springer, 1971.

[20] Salem, R. and Zygmund, A.: Trigonometric series whose terms have random sign. Acta Math. 91 (1954), 245–301.

[21] Schatte, P.: On the asymptotic uniform distribution of sums reduced mod 1. Math. Nachr. 115 (1984), 275–281.

[22] Schatte, P.: On a law of the iterated logarithm for sums mod 1 with application to Benford's law. Prob. Theory Rel. Fields 77 (1988), 167–178.

[23] Takahashi, S.: On the law of the iterated logarithm for lacunary trigonometric series. Tôhoku Math. J. 24 (1972), 319–329.

[24] Takahashi, S.: On the law of the iterated logarithm for lacunary trigonometric series. II. Thoku Math. J. 27 (1975), 391–403.

[25] Weber, M.: Discrepancy of randomly sampled sequences of reals, Math. Nachr. 271 (2004), 105–110.

[26] Williams, D.: Probability with Martingales. Cambridge University Press 1991.