On the discrepancy of random subsequences of $\{n\alpha\}$

István Berkes* and Bence Borda†

Abstract

For irrational α, $\{n\alpha\}$ is uniformly distributed mod 1 in the Weyl sense, and the asymptotic behavior of its discrepancy is completely known. In contrast, very few precise results exist for the discrepancy of subsequences $\{n_k\alpha\}$, with the exception of metric results for exponentially growing (n_k). It is therefore natural to consider random (n_k), and in this paper we give nearly optimal bounds for the discrepancy of $\{n_k\alpha\}$ in the case when the gaps $n_{k+1}-n_k$ are independent, identically distributed, integer valued random variables. As we will see, the discrepancy behavior is determined by a delicate interplay between the distribution of the gaps $n_{k+1}-n_k$ and the rational approximation properties of α. We also point out an interesting critical phenomenon, i.e. a sudden change of the order of magnitude of the discrepancy of $\{n_k\alpha\}$ as the Diophantine type of α passes through a certain critical value.

1 Introduction

An infinite sequence (x_k) of real numbers is called uniformly distributed mod 1 if for every pair a, b of real numbers with $0 \le a < b \le 1$ we have

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} I_{[a,b)}(\{x_k\}) = b - a.$$

Here $\{\cdot\}$ denotes fractional part, and $I_{[a,b)}$ is the indicator function of the interval $[a, b)$. By Weyl's criterion [21], a sequence (x_k) is uniformly distributed mod 1 if and only if

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} e^{2\pi i h x_k} = 0$$

for all integers $h \neq 0$. In particular, the sequence $\{n\alpha\}$ is uniformly distributed mod 1 for any irrational α. It also follows that $\{n_k\alpha\}$ is uniformly distributed mod 1 for all irrational α for $n_k = k^b \log^c k$ $(0 < b < 1, c \in \mathbb{R})$, $n_k = \log^c k$ $(c > 1)$, $n_k = P(k)$,

*A. Rényi Institute of Mathematics, 1053 Budapest, Reáltanoda u. 13-15, Hungary. e-mail: berkes.istvan@renyi.mta.hu. Research supported by NKFIH grant K 125569.

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

where P is a nonconstant polynomial with integer coefficients. See Kuipers and Niederreiter [13] for further examples.

A natural measure of the mod 1 uniformity of an infinite sequence (x_k) is the discrepancy defined by

$$D_N(x_k) := \sup_{0\le a<b\le 1}\left|\frac{1}{N}\sum_{k=1}^{N} I_{[a,b)}(\{x_k\}) - (b-a)\right| \quad (N=1,2,\ldots).$$

By Diophantine approximation theory, the order of magnitude of the discrepancy $D_N(\{n\alpha\})$ is closely connected with the rational approximation properties of α. By a standard definition (see e.g. [13]), the *type* γ of an irrational number α is the supremum of all c such that

$$\liminf_{q\to\infty} q^c\|q\alpha\| = 0,$$

where $\|t\|$ denotes the distance of a real number t from the nearest integer. Then $\gamma \ge 1$ for all irrational α and by classical results (see e.g. [13], Chapter 3, Theorems 3.2 and 3.3) if α has finite type γ, then

$$D_N(\{n\alpha\}) = O(N^{-1/\gamma+\varepsilon}), \qquad D_N(\{n\alpha\}) = \Omega(N^{-1/\gamma-\varepsilon}) \tag{1.1}$$

for any $\varepsilon > 0$. However, the type is a rather crude measure of rational approximation and a more precise characterization can be obtained by using a nondecreasing positive function ψ such that

$$0 < \liminf_{q\to\infty} \psi(q)\|q\alpha\| < \infty. \tag{1.2}$$

Note that e.g. $\psi(q) = \max_{1\le k\le q} 1/\|k\alpha\|$ satisfies (1.2), however ψ is not uniquely determined by α. For the sake of simplicity, in this paper we will focus on the case when (1.2) is satisfied with $\psi(q) = q^\gamma$ for some $\gamma \ge 1$. We shall say in this case that α *has strong type* γ. As a minor change of the proof of (1.1) shows, in this case (1.1) can be improved to

$$D_N(\{n\alpha\}) = O(N^{-1/\gamma}), \qquad D_N(\{n\alpha\}) = \Omega(N^{-1/\gamma})$$

for $\gamma > 1$ and

$$D_N(\{n\alpha\}) = O\left(\frac{\log N}{N}\right)$$

for $\gamma = 1$. In view of Schmidt's theorem (see e.g. [13], p. 109), the last bound is also optimal. Note that for any irrational α (1.2) does not hold with any function $\psi(q) = o(q)$, and that it holds with $\psi(q) = q$ if and only if the partial quotients a_k in the continued fraction of α remain bounded. Such irrational numbers are called "badly approximable".

In contrast to the precise results for $D_N(\{n\alpha\})$ above, much less is known about $D_N(\{n_k\alpha\})$ for general (n_k). By a result of Philipp [15], if (n_k) is a sequence of positive reals with

$$n_{k+1}/n_k \ge q > 1, \quad (k=1,2,\ldots)$$

then $D_N(\{n_k\alpha\})$ satisfies the law of the iterated logarithm, i.e.

$$0 < \limsup_{N\to\infty} \sqrt{\frac{N}{\log\log N}} D_N(\{n_k\alpha\}) < \infty \tag{1.3}$$

for almost all α in the sense of the Lebesgue measure. For general (n_k) growing more slowly, even sharp metric results are not available. R. Baker [2] proved that if (n_k) is an increasing sequence of positive integers, then for any $\varepsilon > 0$

$$D_N(\{n_k\alpha\}) = O\left(N^{-1/2}(\log N)^{3/2+\varepsilon}\right) \tag{1.4}$$

holds for almost all α, but it is not known whether the exponent $3/2$ can be improved. In the case when n_k is a polynomial with integer coefficients in k of degree at least 2, Aistleitner and Larcher [1] proved the lower bound $D_N(\{n_k\alpha\}) = \Omega\left(N^{-1/2-\varepsilon}\right)$, valid for any $\varepsilon > 0$ and almost every α. However, all these are metric results and do not give information on $D_N(\{n_k\alpha\})$ for any specific irrational α.

Thus it is natural to consider random sequences (n_k), and in this paper we consider the case when the gaps $n_{k+1} - n_k$ are independent, identically distributed (i.i.d.) random variables. That is, we are dealing with the discrepancy $D_N(\{S_k\alpha\})$, where $S_k = \sum_{j=1}^{k} X_j$ with i.i.d. random variables $X_1, X_2, \ldots$, i.e. S_k is a random walk. In a recent paper [3] the authors proved the law of the iterated logarithm

$$0 < \limsup_{N\to\infty} \frac{\left|\sum_{k=1}^{N} e^{2\pi i S_k \alpha}\right|}{\sqrt{N \log\log N}} < \infty \quad \text{a.s.}$$

whenever $\exp(2\pi i X_1 \alpha)$ is non-degenerate (i.e. it does not equal a constant with probability 1). Note that a.s. (almost surely) means that the given event has probability 1 in the space of the random walk S_k. From Koksma's inequality ([13], Chapter 2, Corollary 5.1) we thus obtain the following general lower estimate.

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

$$D_N(\{S_k\alpha\}) = \Omega\left(\sqrt{\frac{\log\log N}{N}}\right) \quad \textit{a.s.}$$

The sharpness of Proposition 1.1 follows from a result of Schatte [18], who proved that if

$$\sup_{0\le x\le 1} |\mathbb{P}(\{S_k\alpha\} < x) - x| = O(k^{-5/2}) \tag{1.5}$$

then for all $\alpha \neq 0$ we have

$$0 < \limsup_{N\to\infty} \sqrt{\frac{N}{\log\log N}} D_N(\{S_k\alpha\}) < \infty \quad \text{a.s.} \tag{1.6}$$

Condition (1.5) is satisfied if the distribution of X_1 is absolutely continuous, in which case the convergence speed in (1.5) is exponential. Berkes and Raseta [5] showed that in the absolutely continuous case the LIL (1.6) holds also for the L_p discrepancy of $\{S_k\alpha\}$, $1 \le p < \infty$ and for other functionals of the path $\{S_k\alpha\}, 1 \le k \le N$. Improving results of Schatte [17] and Su [19], in [4] we gave optimal bounds for the quantity on the left hand side of (1.5) in the case when X_1 is an integer valued random variable having a finite variance or having heavy tails, i.e. satisfying

$$P(|X_1| > t) \sim ct^{-\beta} \quad \text{as } t \to \infty \tag{1.7}$$

for some $c > 0$, $0 < \beta < 2$. These results imply that the LIL (1.6) holds also if α has strong type γ and X_1 is an integer valued random variable satisfying (1.7) with $\beta < 2/(5\gamma)$ (see the last paragraph of Subsection 2.1). In this case S_n grows, in a stochastic sense, with the polynomial speed $n^{1/\beta}$ and this result can be considered as the stochastic analogue of Philipp's lacunary result (1.3). On the other hand, the results of [4] also show that (1.5) cannot hold if X_1 has a finite variance, in which case S_n grows at most linearly. In this case the problem of asymptotic behavior of $D_N(\{S_k\alpha\})$ becomes considerably harder and will be studied in the present paper.

Upper bounds for $D_N(\{S_k\alpha\})$ for general random walks in terms of the growth rate of the sums

$$\sum_{h=1}^{H} \frac{1}{h|1-\varphi(2\pi h\alpha)|} \quad \text{and} \quad \sum_{h=1}^{H} \frac{1}{h|1-\varphi(2\pi h\alpha)|^{1/2}}$$

were given in Weber [20] and Berkes and Weber [7]. Here φ denotes the characteristic function of X_1. In particular, in [20] it is shown that if X_1 is integer valued, $S_k/k^{1/\beta}$ converges in distribution to a stable law with parameter $0 < \beta < 1$ and α satisfies $\|q\alpha\| \geq Cq^{-\gamma}$ for every $q \in \mathbb{N}$ with some $\gamma > 1$ and $C > 0$, then

$$D_N(\{S_k\alpha\}) = O\left(N^{-1/(1+\gamma)} \log^{2+\varepsilon} N\right) \quad \text{a.s.} \tag{1.8}$$

for any $\varepsilon > 0$. The same upper bound holds if instead of the distributional convergence of $S_k/k^{1/\beta}$ we assume $\mathbb{E}X_1 \neq 0$ and $\mathbb{E}|X_1| < \infty$. For nearly optimal improvements of this estimate, see Propositions 1.2 and 2.1 below.

The main focus of this paper is to study the discrepancy of $\{S_k\alpha\}$ in the case when X_1 is an integer valued random variable, and α is irrational. The most interesting case is $X_1 > 0$, when $\{S_k\alpha\}$ is in fact a random subsequence of $\{n\alpha\}$, but in general we will allow X_1 to take negative integers as well. Before we formulate our general results, we discuss here the simple special case when X_1 takes the values 1 and 2 with probability 1/2-1/2. The corresponding sequence $\{S_k\alpha\}$ is arguably the simplest random subsequence of $\{n\alpha\}$.

Proposition 1.2. *Let $X_1, X_2, \ldots$ be i.i.d. random variables such that $\mathbb{P}(X_1 = 1) = \mathbb{P}(X_1 = 2) = 1/2$, let $S_k = \sum_{j=1}^{k} X_j$, and let $\alpha \in \mathbb{R}$ be irrational.*

(i) If $\|q\alpha\| \geq Cq^{-2}$ for every $q \in \mathbb{N}$ with some constant $C > 0$, then $D_N = D_N(\{S_k\alpha\})$ satisfies

$$D_N = O\left(\sqrt{\frac{\log\log N}{N}} \log N\right), \quad D_N = \Omega\left(\sqrt{\frac{\log\log N}{N}}\right) \quad \text{a.s.}$$

(ii) If $0 < \liminf_{q\to\infty} q^{\gamma} \|q\alpha\| < \infty$ with some $\gamma > 2$, then $D_N = D_N(\{S_k\alpha\})$ satisfies

$$D_N = O\left(\left(\frac{\log\log N}{N}\right)^{1/\gamma}\right), \quad D_N = \Omega\left(\frac{1}{N^{1/\gamma}}\right) \quad \text{a.s.}$$

For an irrational α with strong type γ, the estimates in (i) hold if $1 \leq \gamma \leq 2$, while those in (ii) hold if $\gamma > 2$. Thus the behavior of $D_N(\{S_k\alpha\})$ changes at the

critical value $\gamma = 2$. It would not be difficult to generalize (ii) for an irrational α satisfying (1.2) with an arbitrary $\psi(q)$ increasing faster than q^2. In this case the estimates for $D_N(\{S_k\alpha\})$ would be given in terms of the inverse function ψ^{-1}.

The estimates in (i) apply to every algebraic irrational α, as well as to almost every α in the sense of the Lebesgue measure. Indeed, a celebrated theorem of Roth [16] states that any algebraic irrational α satisfies $\|q\alpha\| \geq Cq^{-(1+\varepsilon)}$ with some constant $C = C(\alpha, \varepsilon) > 0$, where $\varepsilon > 0$ is arbitrary. Furthermore, according to the Jarník–Besicovitch theorem [8] the set of all $\alpha \in \mathbb{R}$ for which $\liminf_{q\to\infty} q^\gamma \|q\alpha\| < \infty$ has Hausdorff dimension $1/\gamma$. Thus except for a set of Hausdorff dimension $1/2$ (and hence Lebesgue measure 0), every $\alpha \in \mathbb{R}$ satisfies the Diophantine condition in (i).

Note that the exponent 1 of the log in the upper estimate in (i) is smaller than the exponent $3/2$ in Baker's estimate (1.4), and thus random sequences give a better discrepancy bound.

2 Results

2.1 Heavy-tailed distributions

Suppose that the random variable X_1 has a "heavy-tailed" distribution, i.e. $\mathbb{E}X_1^2 = \infty$. For the sake of simplicity, we only formulate a result for random variables whose tail distribution is a power function.

Proposition 2.1. *Let $X_1, X_2, \dots$ be integer valued i.i.d. random variables such that $\mathbb{P}(|X_1| \geq x) \sim cx^{-\beta}$ as $x \to \infty$ with some constants $0 < \beta < 2$ and $c > 0$, and assume that*

$$\lim_{x\to\infty} \frac{\mathbb{P}(X_1 > x)}{\mathbb{P}(|X_1| > x)}$$

exists. In the case $1 < \beta < 2$ suppose, moreover, that $\mathbb{E}X_1 = 0$. Let $S_k = \sum_{j=1}^k X_j$, and let $\alpha \in \mathbb{R}$ be irrational.

(i) If $\|q\alpha\| \geq Cq^{-2/\beta}$ for every $q \in \mathbb{N}$ with some constant $C > 0$, then $D_N = D_N(\{S_k\alpha\})$ satisfies

$$D_N = O\left(\sqrt{\frac{\log\log N}{N}}\log N\right), \quad D_N = \Omega\left(\sqrt{\frac{\log\log N}{N}}\right) \quad a.s.$$

(ii) If $0 < \liminf_{q\to\infty} q^\gamma \|q\alpha\| < \infty$ with some $\gamma > 2/\beta$, then $D_N = D_N(\{S_k\alpha\})$ satisfies

$$D_N = O\left(\left(\frac{\log\log N}{N}\right)^{1/(\beta\gamma)}\right), \quad D_N = \Omega\left(\frac{1}{N^{1/(\beta\gamma)}}\right) \quad a.s.$$

Here we have a similar dichotomy as in Proposition 1.2, the critical value of γ being $2/\beta$. Again, it would not be difficult to generalize (ii) for an irrational α satisfying (1.2) with an arbitrary $\psi(q)$ increasing faster than $q^{2/\beta}$. Similarly, we could derive estimates for random variables with tail distribution $\mathbb{P}(|X_1| \geq x) \sim \phi(x)$, where $\phi(x)$ is not necessarily a power function. In this more general situation

the critical order of magnitude of $\psi(q)$, where the behavior of D_N changes, would not necessarily be a power function.

Note that the estimates in (i) apply to every algebraic irrational α, as well as to almost every α in the sense of the Lebesgue measure.

Proposition 2.1 e.g. applies to the positive integer valued random variable X_1 with $\mathbb{P}(X_1 = n) = c_\beta/n^{1+\beta}$, $n = 1, 2, \dots$, where $0 < \beta \le 1$. This way we obtain a random subsequence $S_k\alpha$ of $n\alpha$ increasing roughly at the polynomial speed $k^{1/\beta}$. More precisely, $S_k = O\left(k^{1/\beta+\varepsilon}\right)$ a.s. holds for any $\varepsilon > 0$ but not for $\varepsilon = 0$ (see e.g. [14], Theorem 6.9).

In conclusion we note that Schatte's LIL under (1.5) and Theorem 1.4 of our previous paper [4] imply that if in statement (i) of Proposition 2.1 we replace the assumption $\|q\alpha\| \ge Cq^{-2/\beta}$ by $\|q\alpha\| \ge Cq^{-2/(5\beta)+\varepsilon}$ with some $\varepsilon > 0$, then, under mild additional technical assumptions on the distribution of X_1, in the conclusion

$$D_N = O\left(\sqrt{\frac{\log\log N}{N}}\log N\right) \quad \text{a.s.}$$

the factor $\log N$ can be dropped, resulting in a sharp LIL bound. Whether this is true under the original assumption remains open.

2.2 The case $\mathbb{E}X_1^2 < \infty$, $\mathbb{E}X_1 = 0$

The previous result deals with the case $\mathbb{E}X_1^2 = \infty$, and covers the typical case when the tails of X_1 decrease with speed $x^{-\beta}$, $0 < \beta < 2$. Next, we consider the case $\mathbb{E}X_1^2 < \infty$. As we will see, the results are substantially different according as $\mathbb{E}X_1$ equals 0 or not, and we start with the easier case $\mathbb{E}X_1 = 0$.

Proposition 2.2. *Let $X_1, X_2, \dots$ be integer valued i.i.d. random variables such that $\mathbb{E}X_1 = 0$ and $\mathbb{E}X_1^2 < \infty$, let $S_k = \sum_{j=1}^k X_j$, and let $\alpha \in \mathbb{R}$ be irrational.*

(i) If $\|q\alpha\| \ge Cq^{-1}$ for every $q \in \mathbb{N}$ with some constant $C > 0$, then $D_N = D_N(\{S_k\alpha\})$ satisfies

$$D_N = O\left(\sqrt{\frac{\log\log N}{N}}\log^2 N\right), \quad D_N = \Omega\left(\sqrt{\frac{\log\log N}{N}}\right) \quad \text{a.s.}$$

(ii) If $0 < \liminf_{q\to\infty} q^\gamma \|q\alpha\| < \infty$ with some $\gamma > 1$, then $D_N = D_N(\{S_k\alpha\})$ satisfies

$$D_N = O\left(\left(\frac{\log\log N}{N}\right)^{1/(2\gamma)}\right), \quad D_N = \Omega\left(\frac{1}{N^{1/(2\gamma)}}\right) \quad \text{a.s.}$$

The dichotomy is less pronounced here than in the previous propositions. Formally, the critical value is now $\gamma = 1$. Thus (i) only applies to badly approximable irrationals, but not to almost every α.

Note that the factor $\log^2 N$ in the upper estimate in (i) is greater than the factor $(\log N)^{3/2+\varepsilon}$ in Baker's bound (1.4). However, Baker's bound does not apply to $\{S_k\alpha\}$, since $\mathbb{E}X_1 = 0$ implies that S_k cannot be an increasing sequence. Additionally, the set of all badly approximable α is of measure 0, and Baker's estimate provides no information on what happens in such sets. As more than one result in our paper shows, discrepancy estimates in zero sets can be much worse than the "typical" behavior.

2.3 The case $\mathbb{E}X_1^2 < \infty$, $\mathbb{E}X_1 \neq 0$

Finally, let us consider the case $\mathbb{E}X_1^2 < \infty$, $\mathbb{E}X_1 \neq 0$. The relation $\mathbb{E}X_1 \neq 0$ holds in particular if $X_1 > 0$, when the sequence S_k is increasing with probability 1, a natural situation since in this case $\{S_k\alpha\}$ is a random subsequence of $\{n\alpha\}$. As we will see, this case is considerably more involved than the previous ones, and we can prove almost tight estimates for the discrepancy only for certain special distributions, such as Proposition 1.2 in Section 1.

In Section 3.2 we will see further examples for which Proposition 1.2 holds. For example, we will see that this is the case if $\mathbb{P}(X_1 = a) = \mathbb{P}(X_1 = b) = 1/2$ for some $a, b \in \mathbb{Z}$, $a \not\equiv b \pmod 2$, and also if $\mathbb{E}|X_1| < 2\mathbb{P}(X_1 = 1)$. However, we do not have a complete characterization of distributions for which the estimates in Proposition 1.2 are valid. In the (admittedly most interesting) case $\mathbb{E}X_1^2 < \infty$, $\mathbb{E}X_1 \neq 0$, for an irrational α of strong type $\gamma > 1$ in general we only know that $D_N(\{S_k\alpha\})$ is, up to logarithmic factors, at most $N^{-1/(\gamma+1)}$ because of (1.8), and at least $N^{-\tau}$ with $\tau = \min\{1/2, 1/\gamma\}$ because of Proposition 1.1 and Lemma 6.1 below. Thus there is a gap between the exponents of N in the upper and lower estimates, and the precise exponent remains open.

2.4 Main theorem

As we have seen, the order of magnitude of the discrepancy $D_N(\{S_k\alpha\})$ depends sensitively on the distribution of X_1 and the Diophantine properties of α. Theorem 2.3 below, which is the main result of our paper, provides criteria in terms of the characteristic function φ of X_1. As we will see, these criteria cover all mentioned classes and actually more.

Theorem 2.3. *Let $X_1, X_2, \dots$ 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 irrational such that $\|q\alpha\| \geq Cq^{-\gamma}$ for every $q \in \mathbb{N}$ with some constants $\gamma \geq 1$ and $C > 0$.*

(i) Suppose there exist real numbers $0 < \beta \leq 2$, $c > 0$ and an integer $d > 0$ such that for any $x \in \mathbb{R}$

$$1 - |\varphi(2\pi x)| \geq c\|dx\|^\beta. \tag{2.1}$$

Then, with $s = 1$ if $0 < \beta < 2$, and $s = 2$ if $\beta = 2$

$$D_N(\{S_k\alpha\}) = \begin{cases} O\left(\sqrt{\frac{\log\log N}{N}}\log^s N\right) & \text{a.s. if } 1 \leq \gamma \leq \frac{2}{\beta}, \\ O\left(\left(\frac{\log\log N}{N}\right)^{1/(\beta\gamma)}\right) & \text{a.s. if } \gamma > \frac{2}{\beta}. \end{cases} \tag{2.2}$$

(ii) Suppose there exist a real number $c > 0$ and an integer $d > 0$ such that for any $x, y \in \mathbb{R}$

$$|\varphi(2\pi x) - \varphi(2\pi y)| \geq c\|d(x-y)\|. \tag{2.3}$$

Then

$$D_N(\{S_k\alpha\}) = \begin{cases} O\left(\sqrt{\frac{\log\log N}{N}}\log N\right) & \text{a.s. if } 1 \leq \gamma \leq 2, \\ O\left(\left(\frac{\log\log N}{N}\right)^{1/\gamma}\right) & \text{a.s. if } \gamma > 2. \end{cases} \tag{2.4}$$

Conditions (2.1) and (2.3) are not standard in probability theory, therefore we offer some insight into their behavior in Section 3.2. As we will see in Proposition 3.2 (i), Theorem 2.3 (i) with $\beta = 2$ applies to any non-degenerate integer valued X_1, making it our most general upper estimate.

Although we did not assume in Theorem 2.3 that X_1 is integer valued, and indeed there exist non-integer valued distributions satisfying (2.1) or (2.3), the estimates, while valid, might be far from optimal in the non-integral case. Note that the upper bounds in Proposition 1.2 will follow from Theorem 2.3 (ii); the upper bounds in Proposition 2.1 will be a corollary of Theorem 2.3 (i) with $0 < \beta < 2$; finally, the upper bounds in Proposition 2.2 will be deduced from Theorem 2.3 (i) with $\beta = 2$. The lower bounds in Propositions 1.2, 2.1 and 2.2 are either a special case of Proposition 1.1, or follow from a simple argument based on the growth rate of S_k, see Lemmas 6.1 and 6.2 below.

Our proof of Theorem 2.3 is based on the Erdős–Turán inequality, which states that for any sequence (x_k) of reals and any $H \in \mathbb{N}$

$$D_N(x_k) \le C\left(\frac{1}{H} + \sum_{h=1}^{H} \frac{1}{h}\left|\frac{1}{N}\sum_{k=1}^{N} e^{2\pi i h x_k}\right|\right) \tag{2.5}$$

with a universal constant $C > 0$. The free parameter H can be chosen arbitrarily to optimize the estimate. Note that the same exponential sum shows up in Weyl's criterion. To estimate $D_N(\{S_k\alpha\})$, we therefore need to study

$$\sum_{k=1}^{N} e^{2\pi i S_k h\alpha}, \tag{2.6}$$

and this is why it was natural to state the conditions of Theorem 2.3 in terms of the characteristic function φ of X_1. The same approach was followed in Weber [20] and Berkes and Weber [7], which were the starting point for our investigations. The various arithmetic and metric upper bounds for $D_N(\{S_k\alpha\})$ in [20] and [7] were based on estimates for the second and fourth moments of (2.6). The improvements in the present paper depend on sharp asymptotic estimates for the $2p$-th moments of (2.6) for $p = O(\log\log N)$, a technique going back to Erdős and Gál [10] and which, as we will see, presents considerable combinatorial difficulties. A crucial ingredient of the argument will be a sharp estimate for Diophantine sums

$$\sum_{h=1}^{H} \frac{1}{h\|h\alpha\|^b} \quad (0 < b \le 1)$$

(see Proposition 4.1 and Corollary 4.3), which has some interest on its own.

3 The moments of an exponential sum

Let $X_1, X_2, \dots$ be i.i.d. random variables, $S_k = \sum_{j=1}^{k} X_j$ and $\alpha \in \mathbb{R}$. In this Section we estimate the moments

$$\mathbb{E}\left|\sum_{k=m+1}^{m+n} e^{2\pi i S_k \alpha}\right|^{2p} \tag{3.1}$$

where $p \geq 1$ is an integer. The order of magnitude of (3.1) depends on a delicate interplay between the distribution of the random variable X_1 and the value of α. Our main focus is when X_1 is integer valued, and α is irrational.

To get a basic understanding of (3.1), consider the simplest case $p = 1$. Expanding the square we get

$$\mathbb{E}\left|\sum_{k=m+1}^{m+n} e^{2\pi i S_k \alpha}\right|^2 = \sum_{k_1,k_2=m+1}^{m+n} \mathbb{E}e^{2\pi i (S_{k_1}-S_{k_2})\alpha}.$$

We need to decompose this sum into three parts, according to the cases $k_1 = k_2$, $k_1 < k_2$ and $k_1 > k_2$. The terms with $k_1 = k_2$ are simply 1. In the other two cases, using the independence of $X_1, X_2, \ldots$ we have

$$\mathbb{E}e^{2\pi i (S_{k_1}-S_{k_2})\alpha} = \begin{cases} \varphi(-2\pi\alpha)^{k_2-k_1} & \text{if } k_1 < k_2, \\ \varphi(2\pi\alpha)^{k_1-k_2} & \text{if } k_1 > k_2. \end{cases} \tag{3.2}$$

It is now easy to sum over all pairs $m+1 \leq k_1, k_2 \leq m+n$ and obtain an explicit formula for (3.1) in the case $p = 1$.

The basic tool for handling the case $p > 1$ is a generalization of the decomposition above which makes an evaluation of the terms similar to (3.2) possible. The number of cases will obviously be much larger than 3, in fact it will be almost as large as $(2p)^{2p}$.

We are ultimately interested in the discrepancy of the sequence $\{S_k\alpha\}$. To use (2.5) with $x_k = S_k\alpha$ for a specific α, we therefore need to estimate (3.1) not only for α, but for every integral multiple of α as well. The main difficulty of this Section is thus that our estimate of (3.1) cannot contain any implied constant depending on α, it needs to be completely explicit.

3.1 Two estimates of the moments

We now prove two estimates of (3.1) under two different conditions on the distribution of X_1. In the proofs we will often use the fact that $\|\cdot\|$ is symmetric and subadditive, i.e. $\|-x\| = \|x\|$ and $\|x+y\| \leq \|x\|+\|y\|$ hold for any $x, y \in \mathbb{R}$, and that the characteristic function φ of any probability distribution satisfies $\varphi(-x) = \bar{\varphi}(x)$ and $|\varphi(x)| \leq 1$ for any $x \in \mathbb{R}$.

Proposition 3.1. *Let $X_1, X_2, \ldots$ be i.i.d. random variables with characteristic function φ, and let $S_k = \sum_{j=1}^{k} X_j$.*

(i) Suppose that there exist real constants $0 < \beta \leq 2$, $c > 0$ and $d > 0$ such that for any $x \in \mathbb{R}$ (2.1) holds. For any $\alpha \in \mathbb{R}$ such that $d\alpha \notin \mathbb{Z}$, and any integers $m \geq 0$, $n \geq 1$ and $p \geq 1$

$$\mathbb{E}\left|\sum_{k=m+1}^{m+n} e^{2\pi i S_k \alpha}\right|^{2p} \leq (8p)^{2p} \max_{1\leq r\leq p} \frac{n^r}{r!\left(c\,\|d\alpha\|^{\beta}\right)^{2p-r}}. \tag{3.3}$$

(ii) Suppose that there exist real constants $c > 0$ and $d > 0$ such that for any $x, y \in \mathbb{R}$ (2.3) holds. For any $\alpha \in \mathbb{R}$ such that $d\alpha \notin \mathbb{Z}$, and any integers

$m \geq 0$, $n \geq 1$ *and* $p \geq 1$

$$\mathbb{E}\left|\sum_{k=m+1}^{m+n} e^{2\pi i S_k \alpha}\right|^{2p} \leq (4p)^{2p} \sum_{r=0}^{p} \frac{n^r}{r!\left(c\left\|d\alpha\right\|\right)^{2p-r}}. \tag{3.4}$$

Proof. Let us expand the power to obtain

$$\mathbb{E}\left|\sum_{k=m+1}^{m+n} e^{2\pi i S_k \alpha}\right|^{2p} = \sum_{k_1,k_2,\ldots,k_{2p}=m+1}^{m+n} \mathbb{E} e^{2\pi i (S_{k_1} - S_{k_2} + \cdots + S_{k_{2p-1}} - S_{k_{2p}})\alpha}. \tag{3.5}$$

In order to compute the expected value, we need to write the exponent as a sum of independent random variables. To this end, let us say that $P = (P_1, P_2, \ldots, P_s)$ is an ordered partition of the set $[2p]$, where $[N]$ denotes the set $\{1, 2, \ldots, N\}$ for any $N \in \mathbb{N}$, if $P_1, P_2, \ldots, P_s$ are pairwise disjoint, nonempty subsets of $[2p]$ such that $\bigcup_{j=1}^{s} P_j = [2p]$. We can associate an ordered partition to every $2p$-tuple $k = (k_1, k_2, \ldots, k_{2p})$ in a natural way: if

$$\{k_1, k_2, \ldots, k_{2p}\} = \{\ell_1, \ell_2, \ldots, \ell_s\} \tag{3.6}$$

with $\ell_1 < \ell_2 < \cdots < \ell_s$, then for any $1 \leq j \leq s$ let

$$P_j(k) = \{i \in [2p] \ : \ k_i = \ell_j\}.$$

Then $P(k) = (P_1(k), P_2(k), \ldots, P_s(k))$ is an ordered partition of $[2p]$. In other words, the numbers $k_1, k_2, \ldots, k_{2p}$ are written in increasing order as $\ell_1 < \ell_2 < \cdots < \ell_s$ (note $s \leq 2p$ where we may or may not have equality since $k_1, k_2, \ldots, k_{2p}$ need not be distinct). $P_1(k)$ denotes the set of indices i such that k_i is the smallest, $P_2(k)$ denotes the set of indices i such that k_i is the second smallest etc. We will decompose the sum in (3.5) according to the value of $P(k)$. For any given ordered partition P of $[2p]$ let

$$S(P) = \sum_{\substack{k_1,k_2,\ldots,k_{2p}=m+1 \\ P(k)=P}}^{m+n} \mathbb{E} e^{2\pi i (S_{k_1} - S_{k_2} + \cdots + S_{k_{2p-1}} - S_{k_{2p}})\alpha}.$$

Let us now fix an ordered partition $P = (P_1, P_2, \ldots, P_s)$ of $[2p]$. Let k be such that $P(k) = P$, and let $\ell_1 < \ell_2 < \cdots < \ell_s$ be as in (3.6). We have

$$S_{k_1} - S_{k_2} + \cdots + S_{k_{2p-1}} - S_{k_{2p}} = \varepsilon_1 S_{\ell_1} + \varepsilon_2 S_{\ell_2} + \cdots + \varepsilon_s S_{\ell_s}$$

where $\varepsilon_j = \sum_{i \in P_j} (-1)^{i+1}$ for any $1 \leq j \leq s$. Since $\ell_1 < \ell_2 < \cdots < \ell_s$, it is now easy to write this as a sum of independent random variables:

$$\varepsilon_1 S_{\ell_1} + \varepsilon_2 S_{\ell_2} + \cdots + \varepsilon_s S_{\ell_s} = c_1 \sum_{t=1}^{\ell_1} X_t + c_2 \sum_{t=\ell_1+1}^{\ell_2} X_t + \cdots + c_s \sum_{t=\ell_{s-1}+1}^{\ell_s} X_t$$

where $c_j = \varepsilon_j + \varepsilon_{j+1} + \cdots + \varepsilon_s$. Note that $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_s$ and $c_1, c_2, \ldots, c_s$ depend only on the fixed ordered partition P. Therefore

$$\mathbb{E} e^{2\pi i (S_{k_1} - S_{k_2} + \cdots + S_{k_{2p-1}} - S_{k_{2p}})\alpha} = \varphi(2\pi c_1 \alpha)^{\ell_1} \varphi(2\pi c_2 \alpha)^{\ell_2 - \ell_1} \cdots \varphi(2\pi c_s \alpha)^{\ell_s - \ell_{s-1}},$$

and

$$S(P) = \sum_{m+1 \le \ell_1 < \ell_2 < \cdots < \ell_s \le m+n} \varphi(2\pi c_1 \alpha)^{\ell_1} \varphi(2\pi c_2 \alpha)^{\ell_2 - \ell_1} \cdots \varphi(2\pi c_s \alpha)^{\ell_s - \ell_{s-1}}. \quad (3.7)$$

This is the generalization of (3.2) for the case of an arbitrary $p \ge 1$. We are going to estimate (3.7) in two different ways, according to the hypotheses (2.1) and (2.3).

First, we prove (i). Observe that the set

$$B = \left\{ k \in \mathbb{Z} \ : \ \|dk\alpha\| < \frac{1}{2} \|d\alpha\| \right\}$$

does not contain any two consecutive integers. Indeed, if $k, k+1 \in B$, then using the symmetry and the subadditivity of $\|\cdot\|$ we would have

$$\|d\alpha\| \le \|d(k+1)\alpha\| + \|-dk\alpha\| < \frac{1}{2} \|d\alpha\| + \frac{1}{2} \|d\alpha\|,$$

contradiction. Clearly $0 \in B$ and $\pm 1 \notin B$. Consider the set

$$\{1 \le j \le s \ : \ c_j \in B\} = \{j_1, j_2, \ldots, j_r\}$$

where $j_1 < j_2 < \cdots < j_r$. Note that

$$c_1 = \varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_s = \sum_{i=1}^{2p} (-1)^{i+1} = 0 \in B,$$

hence $j_1 = 1$. Since B does not contain any two consecutive integers, for any $1 \le a \le r-1$ we have

$$\pm 1 \ne c_{j_a} - c_{j_{a+1}} = \sum_{j_a \le j < j_{a+1}} \varepsilon_j = \sum_{i \in \bigcup_{j_a \le j < j_{a+1}} P_j} (-1)^{i+1}.$$

Similarly, $\pm 1 \notin B$ implies

$$\pm 1 \ne c_{j_r} = \sum_{j_r \le j \le s} \varepsilon_j = \sum_{i \in \bigcup_{j_r \le j \le s} P_j} (-1)^{i+1}.$$

Therefore $\left| \bigcup_{j_a \le j < j_{a+1}} P_j \right| \ge 2$ and $\left| \bigcup_{j_r \le j \le s} P_j \right| \ge 2$. Using the fact that $P_1, P_2, \ldots, P_s$ is a partition of $[2p]$ we thus obtain

$$2r \le \sum_{a=1}^{r-1} \left| \bigcup_{j_a \le j < j_{a+1}} P_j \right| + \left| \bigcup_{j_r \le j \le s} P_j \right| \le 2p.$$

In other words, $c_j \in B$ for at most p indices $1 \le j \le s$.

Let us now apply the triangle inequality to (3.7). For any $j \ne j_1, j_2, \ldots, j_r$ we have $c_j \notin B$, hence condition (2.1) implies

$$|\varphi(2\pi c_j \alpha)| \le 1 - c \|dc_j \alpha\|^\beta \le 1 - \frac{c}{2^\beta} \|d\alpha\|^\beta.$$

For $j = j_1, j_2, \dots, j_r$ let us use the trivial estimate $|\varphi(2\pi c_j \alpha)| \le 1$. Recall that $j_1 = 1$, which means that we in fact use the trivial estimate on the first factor $\varphi(2\pi c_1 \alpha)^{\ell_1}$. This way we obtain

$$|S(P)| \le \sum_{m+1 \le \ell_1 < \ell_2 < \dots < \ell_s \le m+n} \left(1 - \frac{c}{2^\beta} \|d\alpha\|^\beta\right)^{\sum_{j \ne j_1, j_2, \dots, j_r} (\ell_j - \ell_{j-1})}. \tag{3.8}$$

We need to estimate the number of indices $m+1 \le \ell_1 < \ell_2 < \dots < \ell_s \le m+n$ for which the total exponent is some fixed integer

$$\ell = \sum_{\substack{1 \le j \le s \\ j \ne j_1, j_2, \dots, j_r}} (\ell_j - \ell_{j-1}). \tag{3.9}$$

The special indices $\ell_{j_1}, \ell_{j_2}, \dots, \ell_{j_r}$ can be chosen in $\binom{n}{r} \le n^r/r!$ ways. Given $\ell_{j_1}, \ell_{j_2}, \dots, \ell_{j_r}$, the positive integers $\ell_j - \ell_{j-1}$, $j \ne j_1, j_2, \dots, j_r$ determine all of $\ell_1, \ell_2, \dots, \ell_s$. The number of ways to write ℓ as a sum of $s-r$ nonnegative integers (where the order of the terms matter) is $\binom{\ell+s-r-1}{s-r-1}$, provided $r < s$. The number of indices $m+1 \le \ell_1 < \ell_2 < \dots < \ell_s \le m+n$ for which (3.9) holds is thus at most $n^r/r!\binom{\ell+s-r-1}{s-r-1}$, and so (3.8) gives

$$|S(P)| \le \sum_{\ell=0}^{\infty} \frac{n^r}{r!} \binom{\ell+s-r-1}{s-r-1} \left(1 - \frac{c}{2^\beta} \|d\alpha\|^\beta\right)^\ell.$$

This is in fact a well-known power series which can be obtained by differentiating the geometric series $s-r-1$ times. Hence

$$|S(P)| \le \frac{n^r}{r! \left(\frac{c}{2^\beta} \|d\alpha\|^\beta\right)^{s-r}}$$

if $r < s$, but clearly the same is true if $r = s$ (in which case our method simply estimates the absolute value of each term of (3.7) by 1). Here $s \le 2p$ and $2^{\beta(s-r)} \le 4^{2p}$, therefore

$$|S(P)| \le 4^{2p} \frac{n^r}{r! \left(c \|d\alpha\|^\beta\right)^{2p-r}}.$$

We have seen that $r \le p$ for any P. The number of ordered partitions of $[2p]$ is at most $(2p)^{2p}$, hence summing over all ordered partitions P of $[2p]$ finally shows

$$\mathbb{E} \left| \sum_{k=m+1}^{m+n} e^{2\pi i S_k \alpha} \right|^{2p} = \sum_P S(P) \le (8p)^{2p} \max_{1 \le r \le p} \frac{n^r}{r! \left(c \|d\alpha\|^\beta\right)^{2p-r}}.$$

Next, we prove (ii). To estimate (3.7) under hypothesis (2.3) we will need the following lemma.

Lemma 3.1. *Let $m \ge 0, n \ge 1, s \ge 1$ be integers, and let $\delta > 0$. Consider*

$$f_{m,n,s}(x_1, x_2, \dots, x_s) = \sum_{m+1 \le \ell_1 < \ell_2 < \dots < \ell_s \le m+n} x_1^{\ell_1} x_2^{\ell_2} \cdots x_s^{\ell_s}.$$

For a given $x = (x_1, x_2, \dots, x_s) \in \mathbb{C}^s$ let

(i) $q = q(x)$ *denote the maximum number of pairwise disjoint, nonempty intervals of consecutive integers* $I_1, I_2, \ldots, I_q \subseteq [s]$ *such that* $\left|1 - \prod_{j\in I_r} x_j\right| < \delta$ *for all* $1 \le r \le q$,

(ii) $K = K(x) = \max\left\{\prod_{j=a}^{s} |x_j| \ : \ 1 \le a \le s\right\} \cup \{1\}$.

Then

$$|f_{m,n,s}(x_1, x_2, \ldots, x_s)| \le K^{m+n+1}\left(\frac{2}{\delta}\right)^s \sum_{r=0}^{q} \frac{(\delta n)^r}{r!}.$$

Note that $\delta > 0$ is a free parameter, which can be chosen to optimize the estimate. As $\delta \to 0$, each term of the estimate is increasing, however the highest exponent q of n which shows up in the estimate is decreasing.

Proof. We may assume $x_1, x_2, \ldots, x_s \neq 0$, otherwise $f_{m,n,s}(x_1, x_2, \ldots, x_s) = 0$. We use induction on s. First, let $s = 1$, and consider

$$f_{m,n,1}(x_1) = \sum_{m+1\le \ell_1 \le m+n} x_1^{\ell_1}.$$

If $|1 - x_1| < \delta$, then $q = 1$. Using the triangle inequality and $|x_1| \le K$ we get

$$|f_{m,n,1}(x_1)| \le \sum_{m+1\le \ell_1 \le m+n} K^{\ell_1} \le K^{m+n} n \le K^{m+n+1}\frac{2}{\delta}\left(1 + \delta n\right),$$

as claimed. If $|1 - x_1| \ge \delta$, then $q = 0$. In this case we evaluate $f_{m,n,1}(x_1)$ as a partial sum of a geometric series to obtain

$$|f_{m,n,1}(x_1)| = \left|\frac{x_1^{m+1} - x_1^{m+n+1}}{1 - x_1}\right| \le \frac{K^{m+1} + K^{m+n+1}}{\delta} \le K^{m+n+1}\frac{2}{\delta},$$

as claimed.

Suppose now, that the lemma is true for $s-1$, and let us prove it for $s \ge 2$. Let $x = (x_1, x_2, \ldots, x_s) \in \mathbb{C}^s$, and consider $q = q(x)$ and $K = K(x)$. We will treat the cases $|1 - x_s| < \delta$ and $|1 - x_s| \ge \delta$ separately.

Assume first, that $|1-x_s| < \delta$. By fixing ℓ_s first, and summing over $\ell_1, \ell_2, \ldots, \ell_{s-1}$ we get

$$f_{m,n,s}(x_1, x_2, \ldots, x_s) = \sum_{m+s\le \ell_s \le m+n} x_s^{\ell_s} \sum_{m+1\le \ell_1 < \ell_2 < \cdots < \ell_{s-1} \le \ell_s - 1} x_1^{\ell_1} x_2^{\ell_2} \cdots x_{s-1}^{\ell_{s-1}}.$$

Note that the inner sum is $f_{m,\ell_s - m - 1, s-1}(x_1, x_2, \ldots, x_{s-1})$. Let $x^* = (x_1, x_2, \ldots, x_{s-1}) \in \mathbb{C}^{s-1}$, and consider $q^* = q(x^*)$ and $K^* = K(x^*)$. We have $K^* \le K/|x_s|$ and $q^* = q - 1$. Indeed, we can add the singleton $\{s\}$ to the family of pairwise disjoint, nonempty intervals defining q^*. Applying the triangle inequality and the inductive hypothesis we get

$$\begin{aligned}
|f_{m,n,s}(x_1, x_2, \ldots, x_s)| &\le \sum_{m+s\le \ell_s \le m+n} |x_s|^{\ell_s} |f_{m,\ell_s - m - 1, s-1}(x_1, x_2, \ldots, x_{s-1})| \\
&\le \sum_{m+s\le \ell_s \le m+n} |x_s|^{\ell_s} \left(\frac{K}{|x_s|}\right)^{\ell_s} \left(\frac{2}{\delta}\right)^{s-1} \sum_{r=0}^{q-1} \frac{(\delta(\ell_s - m - 1))^r}{r!}.
\end{aligned}$$

Here $|x_s|^{\ell_s}(K/|x_s|)^{\ell_s} \le K^{m+n+1}$, thus

$$|f_{m,n,s}(x_1,x_2,\dots,x_s)| \le K^{m+n+1}\left(\frac{2}{\delta}\right)^{s-1}\sum_{r=0}^{q-1}\frac{\delta^r}{r!}\sum_{m+s\le\ell_s\le m+n}(\ell_s-m-1)^r.$$

The standard estimate

$$\sum_{m+s\le\ell_s\le m+n}(\ell_s-m-1)^r=\sum_{\ell=s-1}^{n-1}\ell^r\le\frac{n^{r+1}}{r+1}$$

shows

$$|f_{m,n,s}(x_1,x_2,\dots,x_s)| \le K^{m+n+1}\frac{1}{2}\left(\frac{2}{\delta}\right)^{s}\sum_{r=0}^{q-1}\frac{(\delta n)^{r+1}}{(r+1)!}.$$

Reindexing the sum over r finishes the proof of the inductive step in the case $|1-x_s|<\delta$.

Finally, assume $|1-x_s|\ge\delta$. Fixing $m+1\le\ell_1<\ell_2<\cdots<\ell_{s-1}\le m+n-1$ first, and summing over $\ell_{s-1}<\ell_s\le m+n$ we obtain

$$f_{m,n,s}(x_1,x_2,\dots,x_s)=\sum_{m+1\le\ell_1<\ell_2<\cdots<\ell_{s-1}\le m+n-1}x_1^{\ell_1}x_2^{\ell_2}\cdots x_{s-1}^{\ell_{s-1}}\frac{x_s^{\ell_{s-1}+1}-x_s^{m+n+1}}{1-x_s},$$

which yields the recursive formula

$$\begin{aligned}f_{m,n,s}(x_1,x_2,\dots,x_s)=&\frac{x_s}{1-x_s}f_{m,n-1,s-1}(x_1,x_2,\dots,x_{s-1}x_s)\\&-\frac{x_s^{m+n+1}}{1-x_s}f_{m,n-1,s-1}(x_1,x_2,\dots,x_{s-1}).\end{aligned}$$

Let $x'=(x_1,x_2,\dots,x_{s-1}x_s)\in\mathbb{C}^{s-1}$, and consider $q'=q(x')$ and $K'=K(x')$. It is easy to see that $q'\le q$ and $K'\le K$. Applying the inductive hypothesis and using $|x_s/(1-x_s)|\le K/\delta$ we get

$$\left|\frac{x_s}{1-x_s}f_{m,n-1,s-1}(x_1,x_2,\dots,x_{s-1}x_s)\right|\le\frac{K}{\delta}K^{m+n}\left(\frac{2}{\delta}\right)^{s-1}\sum_{r=0}^{q}\frac{(\delta n)^r}{r!}.\tag{3.10}$$

Let $x''=(x_1,x_2,\dots,x_{s-1})\in\mathbb{C}^{s-1}$, and consider $q''=q(x'')$ and $K''=K(x'')$. It is easy to see that $q''\le q$ and $K''\le K/|x_s|$. Applying the inductive hypothesis and using $\left|x_s^{m+n+1}/(1-x_s)\right|\le K|x_s|^{m+n}/\delta$ we get

$$\left|\frac{x_s^{m+n+1}}{1-x_s}f_{m,n-1,s-1}(x_1,x_2,\dots,x_{s-1})\right|\le\frac{K|x_s|^{m+n}}{\delta}\left(\frac{K}{|x_s|}\right)^{m+n}\left(\frac{2}{\delta}\right)^{s-1}\sum_{r=0}^{q}\frac{(\delta n)^r}{r!}.\tag{3.11}$$

Adding (3.10) and (3.11) we finally get

$$|f_{m,n,s}(x_1,x_2,\dots,x_s)| \le K^{m+n+1}\left(\frac{2}{\delta}\right)^{s}\sum_{r=0}^{q}\frac{(\delta n)^r}{r!}.$$

□

Let us now return to (3.7). If $\varphi(2\pi c_j\alpha) = 0$ for some $1 \le j \le s$, then $S(P) = 0$. Otherwise $S(P) = f_{m,n,s}(x_1, x_2, \dots, x_s)$, as in Lemma 3.1 with $x_j = \varphi(2\pi c_j\alpha)/\varphi(2\pi c_{j+1}\alpha)$ for $1 \le j \le s-1$, and $x_s = \varphi(2\pi c_s\alpha)$. First, note that for any $1 \le a \le s$ we have

$$\prod_{j=a}^{s} |x_j| = |\varphi(2\pi c_a\alpha)| \le 1,$$

therefore we have $K = K(x) = 1$. For an interval of consecutive integers $[a,b] \subseteq [s]$ with $1 \le a \le b < s$ condition (2.3) implies

$$\left|1 - \prod_{j\in[a,b]} x_j\right| = \left|1 - \frac{\varphi(2\pi c_a\alpha)}{\varphi(2\pi c_{b+1}\alpha)}\right| \ge |\varphi(2\pi c_a\alpha) - \varphi(2\pi c_{b+1}\alpha)|$$
$$\ge c\,\|d(c_a - c_{b+1})\alpha\| = c\,\|d(\varepsilon_a + \varepsilon_{a+1} + \cdots + \varepsilon_b)\alpha\|\,.$$

Similarly, for an interval of consecutive integers $[a,s] \subseteq [s]$ with $1 \le a \le s$ condition (2.3) implies

$$\left|1 - \prod_{j\in[a,s]} x_j\right| = |1 - \varphi(2\pi c_a\alpha)| = |\varphi(2\pi c_a\alpha) - \varphi(2\pi 0)|$$
$$\ge c\,\|dc_a\alpha\| = c\,\|d(\varepsilon_a + \varepsilon_{a+1} + \cdots + \varepsilon_s)\alpha\|\,.$$

Altogether, for any nonempty interval of consecutive integers $I \subseteq [s]$ we have

$$\left|1 - \prod_{j\in I} x_j\right| \ge c\left\|d\left(\sum_{j\in I}\varepsilon_j\right)\alpha\right\| = c\left\|d\left(\sum_{i\in\bigcup_{j\in I}P_j}(-1)^{i+1}\right)\alpha\right\|. \tag{3.12}$$

Estimate (3.12) gives the idea to choose $\delta = c\,\|d\alpha\|$ in Lemma 3.1. With this choice $\left|1 - \prod_{j\in I} x_j\right| < \delta$ implies that

$$\sum_{i\in\bigcup_{j\in I}P_j}(-1)^{i+1} \ne \pm 1,$$

and so $\left|\bigcup_{j\in I} P_j\right| \ge 2$. Hence if $I_1, I_2, \dots, I_q \subseteq [s]$ are pairwise disjoint, nonempty intervals of consecutive integers such that $\left|1 - \prod_{j\in I_r} x_j\right| < \delta$ for every $1 \le r \le q$, then using the fact that $P_1, P_2, \dots, P_s$ is a partition of $[2p]$, we get

$$2q \le \sum_{r=1}^{q}\left|\bigcup_{j\in I_r} P_j\right| = \left|\bigcup_{j\in I_1\cup I_2\cup\cdots\cup I_r} P_j\right| \le 2p.$$

Thus $q = q(x)$, as in Lemma 3.1 satisfies $q \le p$. Applying Lemma 3.1 with $K = 1$, $q \le p$ and $\delta = c\,\|d\alpha\|$ to (3.7), we obtain

$$|S(P)| \le \left(\frac{2}{c\,\|d\alpha\|}\right)^s \sum_{r=0}^{p}\frac{(c\,\|d\alpha\|\,n)^r}{r!} \tag{3.13}$$

for any ordered partition $P = (P_1, P_2, \ldots, P_s)$ of $[2p]$. Here $s \leq 2p$. Since the number of ordered partitions of $[2p]$ is at most $(2p)^{2p}$, summing (3.13) over all ordered partitions P of $[2p]$ finishes the proof of (ii):

$$\mathbb{E}\left|\sum_{k=m+1}^{m+n} e^{2\pi i S_k \alpha}\right|^{2p} = \sum_P S(P) \leq (2p)^{2p} \left(\frac{2}{c\,\|d\alpha\|}\right)^{2p} \sum_{r=0}^{p} \frac{(c\,\|d\alpha\|\,n)^r}{r!}.$$

□

3.2 Examples

We were able to estimate the moments (3.1) in Proposition 3.1 under conditions (2.1) and (2.3) for the characteristic function φ of X_1. We now study probability distributions which satisfy such conditions. First of all note that if X_1 is integer valued, then $\varphi(2\pi x)$ is periodic, e.g. 1 is a period. Thus any lower estimate of $1 - |\varphi(2\pi x)|$ and $|\varphi(2\pi x) - \varphi(2\pi y)|$ needs to be periodic as well, which explains the use of the distance from the nearest integer function $\|\cdot\|$. The constant $d > 0$ accounts for the fact that the smallest period of $\varphi(2\pi x)$ or its absolute value might be less than 1.

It is easy to see that (2.1) with some $0 < \beta < 2$ implies $\mathbb{E}X_1^2 = \infty$. Therefore we can only hope to prove (2.1) with $0 < \beta < 2$ for certain "heavy-tailed" distributions. On the other hand, (2.1) with $\beta = 2$ holds in far more general circumstances. The indicator function of the event E will be denoted by I_E.

Proposition 3.2. *Let X_1 be an integer valued random variable with characteristic function φ.*

(i) If X_1 is non-degenerate, then there exist a real number $c > 0$ and an integer $d > 0$ such that for any $x \in \mathbb{R}$ (2.1) holds with $\beta = 2$.

(ii) Let $0 < \beta < 2$. Suppose there exist constants $K, x_0 > 0$ such that for any $x \geq x_0$

$$\mathbb{E}\left(X_1^2 I_{\{|X_1| \leq x\}}\right) \geq K x^{2-\beta}. \tag{3.14}$$

Then there exist a real number $c > 0$ and an integer $d > 0$ such that for for any $x \in \mathbb{R}$ (2.1) holds.

Proof. Let X_2 be a random variable independent from, and with the same distribution as X_1. Then

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

By taking the real part of both sides and using a trigonometric identity we obtain

$$1 - |\varphi(2\pi x)|^2 = \mathbb{E}\left(1 - \cos\left(2\pi x(X_1 - X_2)\right)\right) = 2\mathbb{E}\sin^2\left(\pi x(X_1 - X_2)\right).$$

Let $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \mathbb{E}\sin^2\left(\pi x(X_1 - X_2)\right)$. Since

$$1 - |\varphi(2\pi x)| \geq \frac{1 - |\varphi(2\pi x)|^2}{2} = f(x),$$

it will be enough to find a lower estimate for $f(x)$.

Let $d > 0$ denote the greatest common divisor of the (finite or infinite) support of $X_1 - X_2$. Note that the non-degeneracy of X_1 implies that this support contains a nonzero integer making $d > 0$ well-defined. f is clearly periodic with period $1/d$. It is also easy to see that $f(x) = 0$ if and only if $x(X_1 - X_2) \in \mathbb{Z}$ with probability 1, or equivalently, if and only if x is an integer multiple of $1/d$. Furthermore, f is continuous, which can be seen e.g. from Lebesgue's dominated convergence theorem. Hence to prove an estimate of the form

$$f(x) \geq c \, \|dx\|^\beta \tag{3.15}$$

for some constant $c > 0$ it is enough to prove (3.15) in an open neighborhood of 0.

Applying the estimate $\sin^2(\pi t) \geq 4t^2$, valid for any $|t| \leq 1/2$, with $t = x(X_1 - X_2)$, whenever possible, gives

$$f(x) \geq 4x^2 \mathbb{E}\left((X_1 - X_2)^2 \, I_{\left\{ |X_1 - X_2| \leq \frac{1}{2|x|} \right\}} \right). \tag{3.16}$$

First, we prove (i). We have $\mathbb{E}(X_1 - X_2)^2 > 0$ (possibly infinite), because X_1 is non-degenerate. From the monotone convergence theorem we can see that

$$\mathbb{E}\left((X_1 - X_2)^2 \, I_{\left\{ |X_1 - X_2| \leq \frac{1}{2|x|} \right\}} \right)$$

is greater than a fixed positive constant in an open neighborhood of 0. Therefore (3.16) shows that (3.15) holds with $\beta = 2$ and some $c > 0$ in an open neighborhood of 0, and we are done.

Next, we prove (ii). Let μ denote any median of $|X_1|$, i.e. let $\mathbb{P}(|X_1| \leq \mu) \geq 1/2$ and $\mathbb{P}(|X_1| \geq \mu) \geq 1/2$. If both $2\mu \leq |X_1| \leq 1/(2|x|) - \mu$ and $|X_2| \leq \mu$ hold, then $|X_1 - X_2| \leq 1/(2|x|)$ and $(X_1 - X_2)^2 \geq X_1^2/4$. Therefore

$$(X_1 - X_2)^2 \, I_{\left\{ |X_1 - X_2| \leq \frac{1}{2|x|} \right\}} \geq \frac{X_1^2}{4} I_{\left\{ 2\mu \leq |X_1| \leq \frac{1}{2|x|} - \mu \right\}} I_{\{|X_2| \leq \mu\}}.$$

Taking the expected value and using the definition of a median we obtain the estimate

$$\begin{aligned} \mathbb{E}\left((X_1 - X_2)^2 \, I_{\left\{ |X_1 - X_2| \leq \frac{1}{2|x|} \right\}} \right) &\geq \frac{1}{8} \mathbb{E}\left(X_1^2 I_{\left\{ 2\mu \leq |X_1| \leq \frac{1}{2|x|} - \mu \right\}} \right) \\ &\geq \frac{1}{8} \mathbb{E}\left(X_1^2 I_{\left\{ |X_1| \leq \frac{1}{2|x|} - \mu \right\}} \right) - \frac{\mu^2}{2}. \end{aligned}$$

Equation (3.16) and condition (3.14) thus imply that (3.15) holds with some $c > 0$ in an open neighborhood of 0. □

Next, we study (2.3). For the sake of simplicity, assume that X_1 is integer valued, and $\mathbb{E}|X_1| < \infty$. Because of the periodicity, we may visualize $\varphi(2\pi x)$ as a continuously differentiable, closed curve on the Euclidean plane. It is easy to see that the "self-intersection points" of this curve, i.e. the solutions of the equation $\varphi(2\pi x) = \varphi(2\pi y)$, $x \neq y$ will play an important role. Indeed, $|\varphi(2\pi x) - \varphi(2\pi y)|$ can be small in two different ways: either x and y are close to each other, or they are close to two different self-intersection points of the curve. In the first case a lower estimate linear in $|x - y|$ can be deduced by assuming $\varphi' \neq 0$ anywhere on $\mathbb{R}$. To handle the second case, we will impose a "rationality" and a "linear independence" condition on the self-intersection points.

Proposition 3.3. *Let X_1 be an integer valued random variable with characteristic function φ such that $\mathbb{E}|X_1| < \infty$ and $\varphi' \neq 0$ anywhere on $\mathbb{R}$. Let $p > 0$ denote the smallest period of $\varphi(2\pi x)$. Suppose that the equation $\varphi(2\pi x) = \varphi(2\pi y)$, $x, y \in [0, p)$, $x \neq y$ has finitely many solutions $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$, and that $x_k - y_k \in \mathbb{Q}$ and $\varphi'(2\pi x_k)/\varphi'(2\pi y_k) \notin \mathbb{R}$ for any $k = 1, 2, \ldots, n$. Then there exist a real number $c > 0$ and an integer $d > 0$ such that for any $x, y \in \mathbb{R}$ (2.3) holds.*

Proof. Clearly $p > 0$ is the reciprocal of the greatest common divisor of the (finite or infinite) support of X_1. By considering pX_1 instead, we may therefore assume $p = 1$. Let $d > 0$ be an integer such that $d(x_k - y_k) \in \mathbb{Z}$ for every $k = 1, 2, \ldots, n$.

Assumption $\mathbb{E}|X_1| < \infty$ implies that φ is differentiable, and φ' is uniformly continuous. The periodicity of φ thus shows $|\varphi'| \geq K_0$ for some constant $K_0 > 0$. For any $k = 1, 2, \ldots, n$ the derivatives $\varphi'(2\pi x_k)$ and $\varphi'(2\pi y_k)$ are linearly independent as planar vectors, because $\varphi'(2\pi x_k)/\varphi'(2\pi y_k) \notin \mathbb{R}$. From the equivalence of finite dimensional norms we get that for any $u, v \in \mathbb{R}$

$$|\varphi'(2\pi x_k)u - \varphi'(2\pi y_k)v| \geq K_k \left(|u| + |v|\right) \tag{3.17}$$

holds with some constant $K_k > 0$. Let $K = \min\{K_k \ : \ 0 \leq k \leq n\}$.

A simple corollary of the uniform continuity of φ' is that the convergence

$$\frac{\varphi(2\pi t) - \varphi(2\pi a)}{2\pi t - 2\pi a} \to \varphi'(2\pi a)$$

as $|t - a| \to 0$ is uniform in $t, a \in \mathbb{R}$. In particular, there exists a constant $r > 0$ such that whenever $|t - a| < r$, then

$$\left|\varphi(2\pi t) - \varphi(2\pi a) - \varphi'(2\pi a)(2\pi t - 2\pi a)\right| \leq \pi K |t - a|. \tag{3.18}$$

Consider the compact set

$$C = \left\{(x, y) \in [0, 1]^2 \ : \ \varphi(2\pi x) = \varphi(2\pi y)\right\}.$$

Note that C consists of the diagonal $x = y$, the points $(0, 1)$, $(1, 0)$ and the finite point set (x_k, y_k), $k = 1, 2, \ldots, n$. Let $(x, y) \in [0, 1]^2$ be such that $\operatorname{dist}((x, y), C) < r/2$, where dist denotes the distance of a point from a set. There are three cases: (x, y) is either close to the diagonal, to $(0, 1)$ or $(1, 0)$, or to the point (x_k, y_k) for some $k = 1, 2, \ldots, n$.

First, assume that the distance of (x, y) from the diagonal is less than $r/2$. Then $|x - y| < r$, thus (3.18) with $t = x$ and $a = y$ implies

$$\begin{aligned} |\varphi(2\pi x) - \varphi(2\pi y)| &\geq |\varphi'(2\pi y)| \cdot |2\pi x - 2\pi y| - \pi K |x - y| \\ &\geq \frac{\pi K}{d} |d(x - y)| \geq \frac{\pi K}{d} \left\|d(x - y)\right\|. \end{aligned}$$

Assume next, that the Euclidean distance of (x, y) from $(0, 1)$ is less than $r/2$. Then (3.18) applies with $t = x$ and $a = y - 1$. Using the periodicity of φ we thus obtain

$$\begin{aligned} |\varphi(2\pi x) - \varphi(2\pi y)| &= |\varphi(2\pi x) - \varphi(2\pi(y - 1))| \\ &\geq |\varphi'(2\pi(y - 1))| \cdot |2\pi x - 2\pi(y - 1)| - \pi K |x - (y - 1)| \\ &\geq \frac{\pi K}{d} |d(x - y) + d| \geq \frac{\pi K}{d} \left\|d(x - y)\right\|. \end{aligned}$$

A similar estimate holds when the distance of (x, y) from $(1, 0)$ is less than $r/2$. Finally, assume that the distance of (x, y) from (x_k, y_k) is less than $r/2$ for some $k = 1, 2, \ldots, n$. In this case (3.18) applies with $t = x$ and $a = x_k$, and also with $t = y$ and $a = y_k$. Since $\varphi(2\pi x_k) = \varphi(2\pi y_k)$, we have

$$|\varphi(2\pi x) - \varphi(2\pi y)| \geq \left|\varphi'(2\pi x_k)(2\pi x - 2\pi x_k) - \varphi'(2\pi y_k)(2\pi y - 2\pi y_k)\right| \\ - \pi K|x - x_k| - \pi K|y - y_k|.$$

Applying (3.17) with $u = x - x_k$ and $v = y - y_k$ we obtain

$$|\varphi(2\pi x) - \varphi(2\pi y)| \geq \pi K \left(|x - x_k| + |y - y_k|\right) \\ \geq \frac{\pi K}{d}|d(x - y) - d(x_k - y_k)| \geq \frac{\pi K}{d}\left\|d(x - y)\right\|.$$

Altogether we showed that for any $(x, y) \in [0, 1]^2$ such that $\operatorname{dist}\left((x, y), C\right) < r/2$ we have

$$|\varphi(2\pi x) - \varphi(2\pi y)| \geq \frac{\pi K}{d}\left\|d(x - y)\right\|.$$

Using the compactness of the corresponding set it is easy to see that for any $(x, y) \in [0, 1]^2$ such that $\operatorname{dist}\left((x, y), C\right) \geq r/2$ we have

$$|\varphi(2\pi x) - \varphi(2\pi y)| \geq c' \left\|d(x - y)\right\|$$

with some constant $c' > 0$. Therefore (2.3) is satisfied with $c = \min\left\{\pi K/d, c'\right\}$ for any $(x, y) \in [0, 1]^2$. By the periodicity of φ, (2.3) is hence satisfied for all $x, y \in \mathbb{R}$. □

Corollary 3.4. *Let X_1 be a random variable with characteristic function φ. Suppose that $\mathbb{P}(X_1 = a) = \mathbb{P}(X_1 = b) = 1/2$ with some $a, b \in \mathbb{Z}$, $a \not\equiv b \pmod 2$. Then there exist a real number $c > 0$ and an integer $d > 0$ such that for any $x, y \in \mathbb{R}$ (2.3) holds.*

Proof. We will show that X_1 satisfies the conditions of Proposition 3.3. The characteristic function of X_1 is

$$\varphi(t) = \frac{1}{2}e^{iat} + \frac{1}{2}e^{ibt} = e^{i\frac{a+b}{2}t}\cos\left(\frac{a - b}{2}t\right).$$

First, note that

$$|\varphi'(t)| = \frac{1}{2}\left|ae^{iat} + be^{ibt}\right| \geq \frac{1}{2}\left||a| - |b|\right| \geq \frac{1}{2},$$

therefore $\varphi' \neq 0$ anywhere on $\mathbb{R}$.

Similarly to Proposition 3.3 we may assume that a and b are relatively prime, i.e. that the smallest period of $\varphi(2\pi x)$ is 1. Observe that $a \not\equiv b \pmod 2$ implies that $a - b$ and $a + b$ are also relatively prime.

Consider the equation $\varphi(2\pi x) = \varphi(2\pi y)$, $x \neq y$ equivalent to

$$e^{\pi i(a+b)(x-y)}\cos\left(\pi(a - b)x\right) = \cos\left(\pi(a - b)y\right), \qquad x \neq y. \tag{3.19}$$

We have

$$\frac{\varphi'(2\pi x)}{\varphi'(2\pi y)} = e^{\pi i(a+b)(x-y)}\frac{i(a + b)\cos(\pi(a - b)x) - (a - b)\sin(\pi(a - b)x)}{i(a + b)\cos(\pi(a - b)y) - (a - b)\sin(\pi(a - b)y)}. \tag{3.20}$$

We distinguish between two cases in (3.19): either $\cos(\pi(a-b)x) = \cos(\pi(a-b)y) = 0$, or $\exp(\pi i(a+b)(x-y)) \in \mathbb{R}$. The first case gives finitely many solutions (x_k, y_k) within a period $[0,1)$, each of which satisfies $(a-b)(x_k-y_k) \in \mathbb{Z}$. Since $\sin(\pi(a-b)x_k)$ and $\sin(\pi(a-b)y_k)$ are both ± 1, for these solutions (3.20) simplifies as

$$\frac{\varphi'(2\pi x_k)}{\varphi'(2\pi y_k)} = \pm e^{\pi i(a+b)(x_k-y_k)}.$$

By way of contradiction, suppose this ratio is purely real. Then $(a+b)(x_k-y_k) \in \mathbb{Z}$. Since $a-b$ and $a+b$ are relatively prime, the integrality of $(a-b)(x_k-y_k)$ and $(a+b)(x_k-y_k)$ implies that $x_k - y_k$ is also an integer. This is impossible within a period $x_k, y_k \in [0,1)$.

Finally, suppose $\exp(\pi i(a+b)(x-y)) \in \mathbb{R}$. It is easy to see that in this case (3.19) also gives finitely many solutions (x_ℓ, y_ℓ) in a period $[0,1)$, each of which satisfies $(a+b)(x_\ell - y_\ell) \in \mathbb{Z}$. Since $\exp(\pi i(a+b)(x_\ell - y_\ell)) = \pm 1$, (3.20) is purely real if and only if

$$\begin{aligned} -\cos(\pi(a-b)x_\ell)\sin(\pi(a-b)y_\ell) + \cos(\pi(a-b)y_\ell)\sin(\pi(a-b)x_\ell) \\ = \sin(\pi(a-b)(x_\ell - y_\ell)) = 0, \end{aligned}$$

which is equivalent to $(a-b)(x_\ell - y_\ell) \in \mathbb{Z}$. Since $a-b$ and $a+b$ are relatively prime, $(a+b)(x_\ell - y_\ell) \in \mathbb{Z}$ and $(a-b)(x_\ell - y_\ell) \in \mathbb{Z}$ would imply $x_\ell - y_\ell \in \mathbb{Z}$, which is impossible within a period $x_\ell, y_\ell \in [0,1)$. Therefore the solutions (x_ℓ, y_ℓ) also satisfy $\varphi'(2\pi x_\ell)/\varphi'(2\pi y_\ell) \notin \mathbb{R}$. □

The simplest case in which the "rationality" and the "linear independence" conditions on the self-intersection points of φ in Proposition 3.3 hold, is when φ is a simple closed curve, i.e. when there are no self-intersection points at all. If $X_1 = 1$ a.s., then $\varphi(2\pi x)$ parametrizes the unit circle. Thus if $X_1 = 1$ has a high enough probability, then $\varphi(2\pi x)$ will look like a slightly "deformed" circle, and we can hope that this slight deformation will not introduce any self-intersection points. It is very easy to turn this idea into a precise proof as follows.

Proposition 3.5. *Let X_1 be an integer valued random variable such that $\mathbb{E}|X_1| < 2\mathbb{P}(X_1 = 1)$. Then the characteristic function φ of X_1 satisfies (2.3) with $c = 8\mathbb{P}(X_1 = 1) - 4\mathbb{E}|X_1| > 0$ and $d = 1$.*

Proof. We give a direct proof without using Proposition 3.3. We have

$$\begin{aligned} |\varphi(2\pi x) - \varphi(2\pi y)| &= \left|\mathbb{E}\left(e^{2\pi i X_1 x} - e^{2\pi i X_1 y}\right)\right| \\ &\geq \mathbb{P}(X_1 = 1)|e^{2\pi i x} - e^{2\pi i y}| - \mathbb{E}\left(|e^{2\pi i X_1 x} - e^{2\pi i X_1 y}| I_{\{X_1 \neq 1\}}\right). \end{aligned}$$

Using

$$\begin{aligned} |e^{2\pi i X_1 x} - e^{2\pi i X_1 y}| &\leq |X_1| \cdot |e^{2\pi i x} - e^{2\pi i y}|, \\ \mathbb{E}\left(|X_1| I_{\{X_1 \neq 1\}}\right) &= \mathbb{E}|X_1| - \mathbb{P}(X_1 = 1) \end{aligned}$$

we deduce

$$|\varphi(2\pi x) - \varphi(2\pi y)| \geq (2\mathbb{P}(X_1 = 1) - \mathbb{E}|X_1|)\,|e^{2\pi i x} - e^{2\pi i y}|.$$

Finally, note that

$$|e^{2\pi i x} - e^{2\pi i y}| = 2|\sin(\pi(x-y))| \geq 4\|x-y\|.$$

□

4 A Diophantine sum

To study the discrepancy of the sequence $\{S_k\alpha\}$, we will combine the Erdős–Turán inequality and our estimates for the high moments of an exponential sum in Proposition 3.1. In order to proceed it will be necessary to estimate sums of the form

$$\sum_{h=1}^{H} \frac{1}{h \|h\alpha\|^b} \tag{4.1}$$

where α is a given irrational and $0 < b \leq 1$. Note that in the proof of Theorem 2.3 b will be $\beta/2$ in (i), while b will be $1/2$ in (ii). The behavior of the sum (4.1) depends on the Diophantine approximation properties of α, i.e. on how well α can be approximated by rational numbers with small denominators. These properties are encoded in the continued fraction representation of α, therefore it is natural to use the theory of continued fractions to estimate (4.1).

Recall that any irrational α has a unique continued fraction representation

$$\alpha = [a_0; a_1, a_2, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$$

where a_0 is an integer and a_i is a positive integer for $i \geq 1$. By truncating the infinite continued fraction we obtain the rational numbers

$$\frac{p_n}{q_n} = [a_0; a_1, a_2, \dots, a_{n-1}] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_{n-1}}}}},$$

$n \geq 1$, called the convergents to α. The main relevance of the convergents is that in a certain sense they are the "best" rational approximations of α.

The fact that p_n/q_n is "close" to α implies that $q_n\alpha$ is "close" to an integer (namely p_n). This gives us the intuition that the largest terms of the sum (4.1) are those for which $h = q_n$ for some n. Since $1/(h \|h\alpha\|^b) \geq 1/h$, the best we can hope for is that the contribution of all other terms is at most constant times $\log H$. We can turn this intuition into a precise statement as follows.

Proposition 4.1. *Let $\alpha = [a_0; a_1, a_2, \dots]$ be the continued fraction representation of an irrational number α, and let $p_n/q_n = [a_0; a_1, a_2, \dots, a_{n-1}]$ denote its convergents. For any $0 < b \leq 1$*

$$\sum_{0<h<q_n} \frac{1}{h \|h\alpha\|^b} = O\left(\log^s q_n + \sum_{0<k<n} \frac{1}{q_k \|q_k\alpha\|^b}\right),$$

where $s = 1$ if $0 < b < 1$, and $s = 2$ if $b = 1$. The implied constant depends only on α and b.

In order to prove Proposition 4.1 we need certain facts from the theory of continued fractions. For a proof see any book on continued fractions, e.g. [9].

Proposition 4.2. *The convergents $p_n/q_n = [a_0; a_1, a_2, \dots, a_{n-1}]$ of an arbitrary irrational number $\alpha = [a_0; a_1, a_2, \dots]$ satisfy the following.*

(i) For any $n \geq 2$ we have $\frac{1}{q_{n+1}+q_n} \leq \|q_n\alpha\| = |q_n\alpha - p_n| \leq \frac{1}{q_{n+1}}$.

(ii) For any $n \geq 1$ we have $q_n\alpha - p_n = (-1)^{n+1}|q_n\alpha - p_n|$.

(iii) The denominators of the convergents satisfy the recurrence $q_{n+1} = a_n q_n + q_{n-1}$ with initial conditions $q_1 = 1$, $q_2 = a_1$.

(iv) For any $n \geq 2$ we have $p_n q_{n-1} - q_n p_{n-1} = (-1)^n$. In particular, p_n and q_n are relatively prime.

□

Proof of Proposition 4.1. Let $k \geq 3$, and consider the sum

$$\sum_{q_k \leq h < q_{k+1}} \frac{1}{h \|h\alpha\|^b}. \tag{4.2}$$

Let $\varepsilon_k = q_k\alpha - p_k$. Note that $\|h\alpha\| = \|hp_k/q_k + h\varepsilon_k/q_k\|$. Here hp_k/q_k is an integer multiple of $1/q_k$, and $|h\varepsilon_k/q_k| < q_{k+1}|\varepsilon_k|/q_k \leq 1/q_k$ for any $q_k \leq h < q_{k+1}$. Assumption $k \geq 3$ ensures $q_k \geq 2$. Hence $\|h\alpha\|$ is basically determined by the residue class of hp_k modulo q_k. In light of sign $\varepsilon_k = (-1)^{k+1}$, the residue classes 0 and $(-1)^k$ will require special treatment. It is thus natural to decompose the sum (4.2) using the index sets

$$\begin{aligned}
A &= \{q_k \leq h < q_{k+1} \ : \ hp_k \equiv 0 \pmod{q_k}\}, \\
B &= \left\{q_k \leq h < q_{k+1} \ : \ hp_k \equiv (-1)^k \pmod{q_k}\right\}, \\
C &= \left\{q_k \leq h < q_{k+1} \ : \ hp_k \not\equiv 0, (-1)^k \pmod{q_k}\right\}.
\end{aligned}$$

First, consider the sum over $h \in A$. Since p_k and q_k are relatively prime, A only contains integral multiples of q_k. For any $h = aq_k \in A$, $a \geq 1$ we thus have

$$\|h\alpha\| = \left\| \frac{0}{q_k} + \frac{aq_k\varepsilon_k}{q_k} \right\| = a|\varepsilon_k| = a\|q_k\alpha\|,$$

and therefore

$$\sum_{h \in A} \frac{1}{h\|h\alpha\|^b} \leq \sum_{a=1}^{\infty} \frac{1}{aq_k (a\|q_k\alpha\|)^b} = O\left(\frac{1}{q_k \|q_k\alpha\|^b}\right). \tag{4.3}$$

Next, let us estimate the sum over $h \in B$. By taking the equation $p_k q_{k-1} - q_k p_{k-1} = (-1)^k$ from Proposition 4.2 (iv) modulo q_k, we obtain that the multiplicative inverse of p_k modulo q_k is $(-1)^k q_{k-1}$, hence every element of B is congruent to q_{k-1} modulo q_k. In fact $B = \{aq_k + q_{k-1} \ : \ 1 \leq a \leq a_k - 1\}$, since $a_k q_k + q_{k-1} = q_{k+1}$ is outside the interval $q_k \leq h < q_{k+1}$. Combining Proposition 4.2 (i) and (iii) we deduce the estimate $a_k q_k |\varepsilon_k| \leq 1 - q_{k-1}|\varepsilon_k|$. For any $h = aq_k + q_{k-1} \in B$ we thus have

$$\|h\alpha\| = \left\| \frac{(-1)^k}{q_k} + \frac{h\varepsilon_k}{q_k} \right\| = \frac{1 - (aq_k + q_{k-1})|\varepsilon_k|}{q_k} \geq (a_k - a)|\varepsilon_k|.$$

Therefore

$$\sum_{h\in B}\frac{1}{h\left\|h\alpha\right\|^b}\le\sum_{a=1}^{a_k-1}\frac{1}{aq_k\left(\left(a_k-a\right)\left\|q_k\alpha\right\|\right)^b}=O\left(\frac{1}{q_k\left\|q_k\alpha\right\|^b}\right). \tag{4.4}$$

Finally, we need to estimate the sum over $h\in C$. The congruence conditions in the definition of C imply that for any $h\in C$ we have

$$\left\|h\alpha\right\|=\left\|\frac{hp_k}{q_k}+\frac{h\varepsilon_k}{q_k}\right\|\ge\frac{1}{2}\left\|\frac{hp_k}{q_k}\right\|.$$

For any integer $a\ge 1$ we therefore have

$$\sum_{\substack{aq_k\le h<(a+1)q_k\\ h\in C}}\frac{1}{h\left\|h\alpha\right\|^b}\le\sum_{aq_k<h<(a+1)q_k}\frac{2^b}{aq_k\left\|\frac{hp_k}{q_k}\right\|^b}. \tag{4.5}$$

Since p_k and q_k are relatively prime, as h runs in the interval $aq_k<h<(a+1)q_k$, the numbers hp_k attain each nonzero residue class modulo q_k exactly once. Considering the cases $0<b<1$ and $b=1$ separately, the right hand side of (4.5) can hence be estimated as

$$\frac{2^b}{aq_k}\sum_{j=1}^{q_k-1}\frac{1}{\left\|\frac{j}{q_k}\right\|^b}\le\frac{2\cdot 2^b}{aq_k}\sum_{1\le j\le q_k/2}\frac{1}{\left(\frac{j}{q_k}\right)^b}=O\left(\frac{\log^{s-1}q_k}{a}\right).$$

Summing over $1\le a\le a_k$ we obtain

$$\sum_{h\in C}\frac{1}{h\left\|h\alpha\right\|^b}=O\left(\log^{s-1}q_k\log a_k\right). \tag{4.6}$$

Adding (4.3), (4.4) and (4.6) we get

$$\sum_{q_k\le h<q_{k+1}}\frac{1}{h\left\|h\alpha\right\|^b}=O\left(\log^{s-1}q_k\log a_k+\frac{1}{q_k\left\|q_k\alpha\right\|^b}\right).$$

Summing over $3\le k\le n-1$ we obtain

$$\sum_{0<h<q_n}\frac{1}{h\left\|h\alpha\right\|^b}=\sum_{0<h<q_3}\frac{1}{h\left\|h\alpha\right\|^b}+O\left(\sum_{k=3}^{n-1}\left(\log^{s-1}q_k\log a_k+\frac{1}{q_k\left\|q_k\alpha\right\|^b}\right)\right). \tag{4.7}$$

Here the sum over $0<h<q_3$ is $O(1)$, because q_3 is a constant depending only on α. The recurrence in Proposition 4.2 (iii) shows $q_n\ge a_{n-1}q_{n-1}$, and iterating this inequality we get

$$q_n\ge a_{n-1}a_{n-2}\cdots a_3q_3.$$

Hence $\sum_{k=3}^{n-1}\log^{s-1}q_k\log a_k=O(\log^s q_n)$, and so (4.7) simplifies to

$$\sum_{0<h<q_n}\frac{1}{h\left\|h\alpha\right\|^b}=O\left(\log^s q_n+\sum_{0<k<n}\frac{1}{q_k\left\|q_k\alpha\right\|^b}\right).$$

□

Corollary 4.3. *Let α be irrational and $0 < b \leq 1$. Suppose there exist constants $\gamma \geq 1$ and $C > 0$ such that $\|q\alpha\| \geq Cq^{-\gamma}$ for every $q \in \mathbb{N}$. Then*

$$\sum_{h=1}^{H} \frac{1}{h \|h\alpha\|^b} = \begin{cases} O\left(\log^s H\right) & \text{if } \gamma \leq \frac{1}{b}, \\ O\left(H^{b\gamma-1}\right) & \text{if } \gamma > \frac{1}{b}, \end{cases}$$

where $s = 1$ if $0 < b < 1$, and $s = 2$ if $b = 1$. The implied constants depend only on α, b and γ.

Proof. Let p_n/q_n denote the convergents to α. Consider the two consecutive convergent denominators such that $q_{n-1} \leq H < q_n$. Proposition 4.1 implies

$$\sum_{h=1}^{H} \frac{1}{h \|h\alpha\|^b} = O\left(\log^s q_n + \sum_{0<k<n} \frac{1}{q_k \|q_k\alpha\|^b}\right). \tag{4.8}$$

Proposition 4.2 (i) shows that $Cq_{n-1}^{-\gamma} \leq \|q_{n-1}\alpha\| \leq 1/q_n$. Rearranging we get $q_n \leq q_{n-1}^{\gamma}/C \leq H^{\gamma}/C$. Therefore the first error term in (4.8) satisfies $\log^s q_n = O\left(\log^s H\right)$.

In the second error term in (4.8) we have

$$\frac{1}{q_k \|q_k\alpha\|^b} \leq C^{-b} q_k^{b\gamma-1} = O\left(q_k^{b\gamma-1}\right).$$

If $\gamma \leq 1/b$, then

$$\sum_{0<k<n} \frac{1}{q_k \|q_k\alpha\|^b} = O\left(\sum_{0<k<n} q_k^{b\gamma-1}\right) = O\left(n\right).$$

The recurrence in Proposition 4.2 (iii) shows that q_n is at least as large as the nth Fibonacci number, therefore $n = O(\log q_{n-1}) = O\left(\log H\right)$. Hence (4.8) simplifies to

$$\sum_{h=1}^{H} \frac{1}{h \|h\alpha\|^b} = O\left(\log^s H + \log H\right) = O\left(\log^s H\right).$$

Finally, assume $\gamma > 1/b$. Proposition 4.2 (iii) shows that $q_{k+2} \geq q_{k+1} + q_k \geq 2q_k$. In particular, any interval of the form $\left[2^{\ell}, 2^{\ell+1}\right)$ contains at most 2 convergent denominators. Hence

$$\begin{aligned} \sum_{0<k<n} \frac{1}{q_k \|q_k\alpha\|^b} &= O\left(\sum_{0<k<n} q_k^{b\gamma-1}\right) = O\left(\sum_{\substack{\ell \\ 2^{\ell} \leq q_{n-1}}} \sum_{2^{\ell} \leq q_k < 2^{\ell+1}} q_k^{b\gamma-1}\right) \\ &= O\left(\sum_{\substack{\ell \\ 2^{\ell} \leq H}} 2^{(\ell+1)(b\gamma-1)}\right) = O\left(H^{b\gamma-1}\right). \end{aligned}$$

Thus in this case (4.8) gives

$$\sum_{h=1}^{H} \frac{1}{h \|h\alpha\|^b} = O\left(\log^s H + H^{b\gamma-1}\right) = O\left(H^{b\gamma-1}\right).$$

□

5 Proof of the upper bounds

In what follows, K will denote positive constants, not always the same, depending (at most) on α and the distribution of X_1. We first show

Lemma 5.1. *Let $X_1, X_2, \dots$ and α be as in Theorem 2.3 and assume (2.1). Then we have for any integers $\ell \geq 0$, $p \geq 1$*

$$\| \max_{2^\ell \leq N \leq 2^{\ell+1}} N D_N(\{S_k\alpha\}) \|_{2p} \leq K\Big(2^{\ell(1-\delta)}p^\delta + 2^{\ell/2}\sqrt{p} \sum_{h=1}^{[K2^{(\ell+1)\delta}/p^\delta]} \frac{1}{h\|dh\alpha\|^{\beta/2}}\Big) \tag{5.1}$$

where $\delta = 1/(\beta\gamma)$. If instead of (2.1) we assume (2.3), then (5.1) holds with $\beta = 1$.

Proof. Assume first (2.1). Then by Proposition 3.1 (i) we have for any integers $m \geq 0$, $n \geq 1$, $h \geq 1$ and $p \geq 1$

$$\mathbb{E}\left|\sum_{k=m+1}^{m+n} e^{2\pi i S_k h\alpha}\right|^{2p} \leq (8p)^{2p} \max_{1\leq r\leq p} \frac{n^r}{r!\,(c\|dh\alpha\|^\beta)^{2p-r}}. \tag{5.2}$$

Let

$$H_n = C^{1/\gamma} d^{-1} (cn/p)^{1/(\beta\gamma)}. \tag{5.3}$$

We claim that for any $1 \leq h \leq H_n$ and $0 \leq r < p$ we have

$$\frac{n^r}{r!\,(c\|dh\alpha\|^\beta)^{2p-r}} \leq \frac{n^{r+1}}{(r+1)!\,(c\|dh\alpha\|^\beta)^{2p-r-1}}. \tag{5.4}$$

To see this, we note that (5.4) is equivalent to $r+1 \leq nc\|dh\alpha\|^\beta$ and for $1 \leq h \leq H_n$ and $0 \leq r < p$ we have by (5.3) and the assumptions of Theorem 2.3,

$$\|dh\alpha\|^\beta \geq C^\beta (dh)^{-\beta\gamma} \geq C^\beta (dH_n)^{-\beta\gamma} = p/(cn) \geq (r+1)/(cn).$$

Thus the maximum on the right hand side of (5.2) is reached for $r = p$ and consequently

$$\left\| \sum_{k=m+1}^{m+n} e^{2\pi i S_k h\alpha} \right\|_{2p} \leq K\sqrt{np}\, \frac{1}{\|dh\alpha\|^{\beta/2}} \tag{5.5}$$

for all $m \geq 0$, $n \geq 1$, $p \geq 1$ and $1 \leq h \leq H_n$. Set now

$$D_N(\alpha) = D_N(\{S_k\alpha\}), \quad T_h(N,\alpha) = \sum_{k=1}^{N} e^{2\pi i h S_k \alpha}.$$

By the Erdős–Turán inequality we have

$$N D_N(\alpha) \leq 6\left(\frac{N}{[H_N]} + \sum_{h=1}^{[H_N]} \frac{1}{h} |T_h(N,\alpha)|\right)$$

and consequently

$$\max_{2^\ell \leq N \leq 2^{\ell+1}} N D_N(\alpha) \leq K\Big(2^{\ell(1-\delta)}p^\delta + \sum_{h=1}^{[K2^{(\ell+1)\delta}/p^\delta]} \frac{1}{h} \max_{2^\ell \leq N \leq 2^{\ell+1}} |T_h(N,\alpha)|\Big). \tag{5.6}$$

(Note that $N/[H_N] \sim Kp^\delta N^{1-\delta}$ and thus its maximum for $2^\ell \le N \le 2^{\ell+1}$ is $\le K2^{\ell(1-\delta)}p^\delta$.) By (5.5)

$$\|T_h(N,\alpha)\|_{2p} \le K\sqrt{Np}\frac{1}{\|dh\alpha\|^{\beta/2}}. \tag{5.7}$$

Since the estimate (5.7) remains valid for shifted sums $T_h(N,M,\alpha) = \sum_{k=M+1}^{M+N} e^{2\pi i h S_k \alpha}$ as well, we get by the Erdős–Stechkin inequality

$$\|\max_{2^\ell \le N \le 2^{\ell+1}} T_h(N,\alpha)\|_{2p} \le K2^{\ell/2}\sqrt{p}\frac{1}{\|dh\alpha\|^{\beta/2}}. \tag{5.8}$$

Substituting this in (5.6) it follows that

$$\|\max_{2^\ell \le N \le 2^{\ell+1}} ND_N(\alpha)\|_{2p} \le K\left(2^{\ell(1-\delta)}p^\delta + 2^{\ell/2}\sqrt{p}\sum_{h=1}^{[K2^{(\ell+1)\delta}/p^\delta]}\frac{1}{h\|dh\alpha\|^{\beta/2}}\right),$$

and thus (5.1) is proved under condition (2.1) in Theorem 2.3.

If instead of (2.1) we assume (2.3), the proof of (5.1) is essentially the same as above. In this case in Proposition 3.1 we have (3.4) instead of (3.3) which implies, in view of the monotonicity relation (5.4) that (5.5) remains valid in this case with $\beta = 1$ and a different constant K. The rest of the proof of (5.1) requires no change. □

Proof of Theorem 2.3. Assume first that (2.1) holds. We will deal separately with the cases $\gamma > 2/\beta$ and $1 \le \gamma \le 2/\beta$.

Assume $\gamma > 2/\beta$. Then $\delta < 1/2$ and thus from Lemma 5.1 and Corollary 4.3 we get

$$\begin{aligned}\|\max_{2^\ell \le N \le 2^{\ell+1}} ND_N(\{S_k\alpha\})\|_{2p} &\le K\left(2^{\ell(1-\delta)}p^\delta + 2^{\ell/2}\sqrt{p}\left(2^{(\ell+1)\delta}/p^\delta\right)^{\beta\gamma/2-1}\right)\\ &= K\left(2^{\ell(1-\delta)}p^\delta + 2^{\ell/2}\sqrt{p}\,2^{(\ell+1)(1/2-\delta)}p^{\delta-1/2}\right)\\ &\le K2^{\ell(1-\delta)}p^\delta\end{aligned}$$

for any integers $\ell \ge 0$, $p \ge 1$. Choosing $p \sim \log \ell$ and using the Markov inequality we get for a sufficiently large constant $B > 0$

$$\mathbb{P}\left(\max_{2^\ell \le N \le 2^{\ell+1}} ND_N(\{S_k\alpha\}) \ge B2^{\ell(1-\delta)}p^\delta\right) \le \left(\frac{K2^{\ell(1-\delta)}p^\delta}{B2^{\ell(1-\delta)}p^\delta}\right)^{2p} \le 4^{-2p} \le \ell^{-2}.$$

Using the Borel–Cantelli lemma we get

$$\max_{2^\ell \le N \le 2^{\ell+1}} ND_N(\{S_k\alpha\}) = O\left(2^{\ell(1-\delta)}p^\delta\right) = O\left(2^{\ell(1-\delta)}(\log\log 2^\ell)^\delta\right) \qquad \text{a.s.}$$

proving the second estimate in (2.2).

Assume now $1 \le \gamma \le 2/\beta$. Then $\delta \ge 1/2$ and thus using Lemma 5.1 and Corollary 4.3 we get

$$\|\max_{2^\ell \le N \le 2^{\ell+1}} ND_N(\{S_k\alpha\})\|_{2p} \le K\left(2^{\ell/2}p^\delta + 2^{\ell/2}\sqrt{p}\,\ell^s\right) \le K2^{\ell/2}\ell^s\sqrt{p}$$

for any integers $\ell \geq 1$, $1 \leq p \leq \ell^{s/\delta}$, where $s = 1$ if $0 < \beta < 2$, and $s = 2$ if $\beta = 2$. Choosing again $p \sim \log \ell$ and using the Markov inequality we get for a sufficiently large constant B

$$\mathbb{P}\left(\max_{2^\ell \leq N \leq 2^{\ell+1}} N D_N(\{S_k\alpha\}) \geq B 2^{\ell/2} \ell^s \sqrt{p} \right) \leq 4^{-2p} \leq \ell^{-2}.$$

Hence the Borel–Cantelli lemma yields the first estimate in (2.2).

If in Theorem 2.3 we assume (2.3), the argument is the same, using the fact that in this case by Lemma 5.1 we have relation (5.1) with $\beta = 1$. □

Corollary 3.4 shows that the random variable with distribution $\mathbb{P}(X_1 = 1) = \mathbb{P}(X_1 = 2) = 1/2$ satisfies the conditions of Theorem 2.3 (ii), proving the upper bounds in Proposition 1.2. To see the upper bounds in Proposition 2.1 note that the condition $\mathbb{P}(|X_1| > x) \sim cx^{-\beta}$ clearly implies (3.14), and so according to Proposition 3.2 (ii), Theorem 2.3 (i) applies. Finally, the upper bounds in Proposition 2.2 follow from Theorem 2.3 (i) with $\beta = 2$ and Proposition 3.2 (i).

6 Proof of the lower bounds

We start with proving two general lower bounds of independent interest.

Lemma 6.1. *Let $X_1, X_2, \ldots$ be integer valued random variables, let $S_k = \sum_{j=1}^k X_j$, and let $\alpha \in \mathbb{R}$ be irrational such that $\|q\alpha\| \leq Cq^{-\gamma}$ holds for infinitely many $q \in \mathbb{N}$ with some constants $\gamma \geq 1$ and $C > 0$. Assume that $S_k = O(\psi(k))$ a.s., where $\psi(k)$ is a nondecreasing sequence of positive reals. Then*

$$D_N(\{S_k\alpha\}) = \Omega\left(\psi(N+1)^{-1/\gamma}\right) \quad \text{a.s.} \tag{6.1}$$

Note that here we allow $X_1, X_2, \ldots$ to be degenerate, in which case the sequence (S_n) is a deterministic sequence of integers.

Proof. If $\psi(k) = O(1)$, then the sequence $\{S_k\alpha\}$ attains only finitely many points, and thus $D_N(\{S_k\alpha\}) = \Omega(1)$ a.s. trivially holds. We may therefore assume $\psi(k) \to \infty$ as $k \to \infty$. Let $K > 0$ be a random variable such that $|S_k| \leq K\psi(k)$ for every $k \in \mathbb{N}$.

Let $q \in \mathbb{N}$, $q > (3CK\psi(1))^{1/\gamma}$ be such that $\|q\alpha\| = |q\alpha - p| \leq Cq^{-\gamma}$, where $p = p(q)$ denotes the integer closest to $q\alpha$. Let $N = N(q)$ be the largest positive integer such that $\psi(N) < q^\gamma/(3CK)$, i.e. $\psi(N) < q^\gamma/(3CK) \leq \psi(N+1)$. Note that

$$\left| S_k\alpha - \frac{S_k p}{q} \right| = |S_k| \frac{\|q\alpha\|}{q} \leq K\psi(N) \frac{Cq^{-\gamma}}{q} < \frac{1}{3q}$$

holds for any $k = 1, 2, \ldots, N$. This means that $S_k\alpha$ is in the open neighborhood of some integral multiple of $1/q$ with radius $1/(3q)$. In particular, none of the points $\{S_k\alpha\}$, $k = 1, 2, \ldots, N$ lie in the interval $[1/(3q), 2/(3q)] \subset [0, 1]$. By the definition of discrepancy we thus have

$$D_N(\{S_k\alpha\}) \geq \frac{1}{3q} \geq \frac{1}{3\left(3CK\psi(N+1)\right)^{1/\gamma}}. \tag{6.2}$$

Clearly there are only finitely many $q \in \mathbb{N}$ for which $N(q)$ is a given integer, therefore the existence of infinitely many $q \in \mathbb{N}$ with $\|q\alpha\| \le Cq^{-\gamma}$ implies the existence of infinitely many $N \in \mathbb{N}$ for which (6.2) holds. □

Lemma 6.2. *Let $X_1, X_2, \dots$ be integer valued i.i.d. random variables, put $S_n = \sum_{k=1}^{n} X_k$ and assume that for some $0 < \beta \le 2$, $S_n/n^{1/\beta}$ has a non-degenerate limit distribution. Assume further that $\|q\alpha\| \le Cq^{-\gamma}$ holds for infinitely many $q \in \mathbb{N}$ with some constants $\gamma \ge 1$ and $C > 0$. Then*

$$D_N(\{S_k\alpha\}) = \Omega\left(N^{-1/(\beta\gamma)}\right) \quad a.s. \tag{6.3}$$

If $\mathbb{E}X_1 = 0$, $\mathbb{E}X_1^2 < \infty$, then the assumption made on S_n holds with $\beta = 2$. The same holds if X_1 satisfies

$$\mathbb{P}(|X_1| > x) \sim cx^{-\beta} \text{ as } x \to \infty$$

with some $c > 0$, $0 < \beta < 2$ and

$$\lim_{x\to\infty} \frac{\mathbb{P}(X_1 > x)}{\mathbb{P}(|X_1| > x)}$$

exists, see Feller [11], p. 581.

Proof of Lemma 6.2. We will use a trivial version of the Borel–Cantelli lemma stating that if $A_1, A_2, \dots$ are arbitrary events with $\mathbb{P}(A_k) \ge c$ $(k = 1, 2, \dots)$, then with probability $\ge c$, infinitely many A_k will occur. By the assumptions, there exists an infinite subset H of $\mathbb{N}$ such that $\|q\alpha\| \le Cq^{-\gamma}$ for $q \in H$. For each $q \in H$, let $N = N(q) = [aq^{\beta\gamma}]$, where a is a small constant. Let $M_n = \max_{1\le k\le n} |S_k|$. Since $S_n/n^{1/\beta}$ has a non-degenerate limit distribution, Lemma 2.2 of [12] implies the existence of positive constants C_1, C_2 such that

$$\mathbb{P}(M_n > 2C_1 n^{1/\beta}) \le 2\mathbb{P}(|S_n| > C_1 n^{1/\beta}) \le 1 - C_2$$

for sufficiently large n. Thus letting

$$A_q = \left\{M_{N(q)} \le 2C_1 N(q)^{1/\beta}\right\},$$

we have $\mathbb{P}(A_q) \ge C_2$ for sufficiently large $q \in H$ and thus with probability $\ge C_2$ infinitely many of the A_q, $q \in H$ occur. By the Hewitt–Savage zero-one law (see e.g. [6], p. 64, Corollary 3.50), this is actually true with probability 1. Choose now such a q, then $\|q\alpha\| = |q\alpha - p| \le Cq^{-\gamma}$, where $p = p(q)$ denotes the integer closest to $q\alpha$. Hence for $N = N(q)$ we have for any $1 \le k \le N$

$$\left|S_k\alpha - \frac{S_k p}{q}\right| \le \frac{|S_k|}{q^{\gamma+1}} \le \frac{|M_N|}{q^{\gamma+1}} \le \frac{2C_1 N^{1/\beta}}{q^{\gamma+1}} \le \frac{2C_1 a^{1/\beta}}{q} \le \frac{1}{3q} \tag{6.4}$$

provided a is small enough. Since X_1 is integer valued, the points $S_k p/q$ are integer multiples of $1/q$ and thus by (6.4) the points $S_k\alpha$ $(1 \le k \le N)$ differ from each other by $\ge 1/(3q)$, and consequently

$$D_N(\{S_k\alpha\}) \ge \frac{1}{3q} \ge C_3 N^{-1/(\beta\gamma)}$$

for infinitely many N, as stated. □

With Lemmas 6.1 and 6.2 at hand, the lower bounds in Propositions 1.2 (ii), 2.1 (ii), 2.2 (ii) follow immediately.

References

[1] C. Aistleitner and G. Larcher, Metric results on the discrepancy of sequences $(a_n\alpha)_{n\geq 1}$ modulo one for integer sequences $(a_n)_{n\geq 1}$ of polynomial growth. Mathematika 62 (2016), 478–491.

[2] R. C. Baker, Metric number theory and the large sieve. J. London Math. Soc. 24 (1981), 34–40.

[3] I. Berkes and B. Borda, On the law of the iterated logarithm for random exponential sums. Trans. Amer. Math. Soc., to appear.

[4] I. Berkes and B. Borda, Diophantine approximation and Berry-Esseen bounds. Analysis Math., to appear.

[5] I. Berkes and M. Raseta, On the discrepancy and empirical distribution function of $\{n_k\alpha\}$. Unif. Distr. Theory 10 (2015), 1–17.

[6] L. Breiman, Probability, Second Ed. SIAM, 1992.

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

[8] A. S. Besicovitch, Sets of fractional dimensions IV. J. London Math. Soc. 9 (1934), 126–131.

[9] J. W. S. Cassels, An Introduction to Diophantine Approximation. Cambridge Tracts in Mathematics and Mathematical Physics, no. 45. Cambridge University Press, New York, 1957.

[10] P. Erdős and I. Gál, On the law of the iterated logarithm. Proc. Konink. Nederl. Akad. Wetensch. 58 (1955), 65–84.

[11] W. Feller, An Introduction to Probability Theory and its Applications, Vol II, Second Ed. Wiley, 1971.

[12] N. C. Jain and W. E. Pruitt, Maxima of partial sums of independent random variables. Z. Wahrscheinlichkeitstheorie verw. Geb. 27 (1973), 141–151.

[13] L. Kuipers and H. Niederreiter, Uniform Distribution of Sequences. Pure and Applied Mathematics. Wiley, New York-London-Sydney, 1974.

[14] V. V. Petrov, Limit Theorems of Probability Theory. Sequences of Independent Random Variables. Oxford Studies in Probability, vol. 4. Oxford Science Publications, Clarendon Press, Oxford, 1995.

[15] W. Philipp, A functional law of the iterated logarithm for empirical distribution functions of weakly dependent random variables. Ann. Probability 5 (1977), 319–350.

[16] K. F. Roth, Rational approximations to algebraic numbers, Mathematika, 2 (1955), 1–20.

[17] P. Schatte, On the asymptotic uniform distribution of the n-fold convolution mod 1 of a lattice distribution, Math. Nachr. 128 (1986) 233–241.

[18] P. Schatte, On a uniform law of the iterated logarithm for sums mod 1 and Benfords law. Lithuanian Math. J. 31 (1991), 133–142.

[19] F. E. Su, Convergence of random walks on the circle generated by an irrational rotation, Trans. Amer. Math. Soc. 350 (1998), 3717–3741.

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

[21] H. Weyl: Über die Gleichverteilung von Zahlen mod. Eins, Math. Ann. 77 (1916), 313–352.