Random walks on the circle and measure of irrationality

Bruno Massé

Random walks on the circle and measure of irrationality

Bruno Massé [1]
bruno.masse@univ-littoral.fr

October 29, 2021

Abstract

Let Y_n be the number of attempts needed to get the nth success in a non-stationary sequence of independent Bernoulli trials and denote by α a fixed irrational number. We prove that, under mild conditions on the probabilities of success, the law of the fractional part of αY_n converges weakly to the uniform distribution on $[0, 1)$ whenever α is irrational. We then compute upper bounds of the convergence rates depending on a measure of irrationality of α and on the probabilities of success. As an application, we discuss the mantissa of a^{Y_n} for positive integer a and the mantissa of the nth random Mersenne number generated by the Cramér model of pseudo-primes.

1 Introduction

We denote by U the uniform distribution on $[0, 1)$ and by $\{y\}$ the fractional part of a real y. When dealing with fractional parts it is natural to identify $[0, 1)$ to a circle of radius $(2\pi)^{-1}$. We will then write *circle* $[0, 1)$ to indicate that we equip $[0, 1)$ with the topology generated by the functions f which are continuous in the usual sense and satisfy $\lim_{x\to 1} f(x) = f(0)$. This is crucial for the Weyl criterion and the Erdős-Turán inequality (Lemmas 1 and 2 below) on which all our results rely.

As $n \to +\infty$, the uniform probability measure on the set $\{\{\alpha k\} : k = 1, \dots, n\}$ converges weakly to U if and only if α is irrational [11, p. 8]. For this reason, the sequences $(\alpha n)_n$ with irrational α are said to be uniformly distributed modulo 1. We see them as non-random walks on the circle $[0, 1)$. Consider an irrational number α and a sequence of independent Bernoulli trials whose probabilities of success sum to $+\infty$ and decrease to zero as the process moves forward. Remove from the sequence $(\{\alpha n\})_n$ all the points $\{\alpha k\}$ for which the kth trial fails ($k = 1, 2, \dots$). The remaining points are $\{\alpha Y_1\}, \{\alpha Y_2\}, \dots$, where Y_n denotes the number of attempts needed to get the n-th success. The sequence of random variables $(\{\alpha Y_n\})_n$ is a random walk on $[0, 1)$ whose trajectories are random subsequences of

[1] Univ. Littoral Côte d'Opale, UR 2597, LMPA, Laboratoire de Mathématiques Pures et Appliquées Joseph Liouville, F-62100 Calais, France

Key words and phrases: Modulo 1 distribution, Benford law, Fourier coefficients, Weak convergence, Measure of irrationality.

2010 Mathematics subject classification: 60B10, 11K06, 11J82

$(\{\alpha n\})_n$. The present paper investigates the distribution of the possible values of the nth term of these subsequences.

We prove below that, as $n \to +\infty$, the law of $\{\alpha Y_n\}$ converges weakly to U whenever α is irrational. We then provide some bounds of the convergence rates depending on the *type* of α and the probabilities of success. As applications we discuss the *mantissa* of a^{Y_n} for positive integer a and the mantissa of the nth *random Mersenne number* generated by the Cramér model of pseudo-primes. The law of a random variable, the type of an irrational number, the mantissa of a positive real and the random Mersenne numbers are defined in Section 1.1.

The convergence rate of the law of $\{\alpha Z_n\}$, where Z_n is the sum of n independent and identically distributed random, is examined in [20] and [2]. The involved random variables are subject to certain additional conditions in [2] and take values -1 and 1 with probabilities 1/2 in [20]. In both papers, the bounds depend explicitly on the type of α. In our work the random variables $Y_{n+1} - Y_n$ are not independent and are not identically distributed (except in Section 5) and our bounds depend not only on the type of α but also on the probabilities of success.

Among many other references, relevant background material concerning Uniform Distribution Theory and on Benford's law in connection with Number Theory or Probability Theory is available in [1, 4, 11, 13].

1.1 Definitions and notation

Recall that we denote by U the uniform distribution on $[0, 1)$ and by $\{y\}$ the fractional part of a real y. We will use standard notation: $\lfloor y \rfloor$ for the greatest integer less than or equal to y, $[y]$ for the nearest integer value of y (there is no ambiguity when y is irrational), $\langle y \rangle$ for the distance between y and its nearest integer, p_n for the nth prime number, $\log n$ for the natural logarithm of n, $\log_b a$ for the logarithm to the base b of a and $e_h(x)$ for $\exp(2i\pi hx)$ with $i^2 = -1$.

Let $(X_n)_{n\geq 1}$ be a sequence of independent Bernoulli random variables. We suppose that the probabilities of success $q_n = P(X_n = 1)$ sum to $+\infty$. According to Borel-Cantelli Lemma, this is necessary and sufficient to ensure that $S_n = \sum_{j=1}^n X_j \to +\infty$ almost surely as $n \to +\infty$ and so that the number of trials needed to get the n-th success $Y_n = \min\{N : S_N = n\}$ is almost surely well defined for all n. We set $\kappa(n) = q_1 + \cdots + q_n$ and $\lambda(n) = q_n/\sqrt{\kappa(n-1)}$.

The nth Mersenne number is $2^{p_n} - 1$. If $q_1 = q_2 = 0$ and $q_n = (\log n)^{-1}$ for $n \geq 3$, Y_n is the nth Camér random pseudo-prime [21, p. 91–97] and is denoted by p_n^* below. The sequences of random variables $(p_n^*)_n$ and $(2^{p_n^*} - 1)_n$ will be called in the sequel the *Cramér sequence* and *Mersenne-Cramér sequence* respectively. The Cramér sequence is almost surely equivalent to $(p_n)_n$ [5].

Fix a numeration base $b > 1$. The mantissa in base b of a positive real x is the unique number $\mathcal{M}_b(x) \in [1, b)$ such that $x = \mathcal{M}_b(x)b^m$ for some integer m. The Benford's law in base b is the probability distribution B_b on $[1, b)$ defined by $B_b([1, t)) = \log_b t$ for $t \in [1, b)$. A sequence $(x_n)_n$ of positive real numbers is said to be *Benford in base b* when the uniform probability measure on the set $\{\mathcal{M}_b(x_k) : k = 1, \ldots, n\}$ converges weakly to B_b as $n \to +\infty$.

Following [11, p. 161], we define the *type* $\eta(\alpha)$ of an irrational α by

$$\eta(\alpha) = \sup\{\gamma : \liminf_{h\to+\infty} h^\gamma \langle h\alpha \rangle = 0\}.$$

The greater $\eta(\alpha)$ is, the closer α is to rationals with *reasonable* denominators. An irrational α is said to be *of constant type* if $h\langle h\alpha\rangle > c$ for some constant $c > 0$ and all positive integers h or equivalently if the partial quotients of its continued fraction expansion are bounded [11, p. 122]. Such α is of type 1.

The law of a random variable Z is the unique probability measure Q satisfying $Q(B) = P(Z \in B)$ for every Borel set B.

1.2 Content

Our results on the weak convergence of the laws of $\{\alpha Y_n\}$ and $\mathcal{M}_b(a^{Y_n})$ and on the rates of convergence are stated and compared with existing literature in Section 2. Section 3 collects the main tools used in our proofs; they are all well-known, with the possible exception of Proposition 1. Our proofs are collected in Section 4. Finally, we discuss shortly the accuracy of our bounds is in Section 5.

1.3 Information about Mersenne numbers

The consideration of Mersenne numbers was motivated by the construction of even perfect numbers [18, pp. 75-83]. It is easy to check that if $a^k - 1$ is prime for some positive integers a and k, then it is a Mersenne number. Seven of the first eight Mersenne numbers are prime. However the frequency of primes among the Mersenne numbers seems tiny since the 47th prime Mersenne number is $2^{43\,112\,609} - 1$ [24]. The largest known prime since December 2018 is the Mersenne number $2^{82\,589\,933} - 1$ which has more than 24 million digits in base 10 [24]. Most of the known prime Mersenne numbers have held the record of the largest known prime at a time.

1.4 Information about Benford law

Note that $\{\log_b x\} = \log_b(\mathcal{M}_b(x))$. Thus

$$(\mathcal{M}_b(x) < t) \iff (\{\log_b x\} < \log_b t) \qquad (t \in [1, b)) \tag{1}$$

and so, for any positive random variable Z, $\mathcal{M}_b(Z)$ is distributed following B_b if and only if $\{\log_b Z\}$ is distributed following U and, for positive random variables Z_n $(n = 1, 2, \dots)$, the law of $\mathcal{M}_b(Z_n)$ converges weakly to B_b as $n \to +\infty$ if and only if the law of $\{\log_b Z_n\}$ converges weakly to U. In particular a sequence $(x_n)_n$ is Benford in base b if and only if the sequence $(\log_b(x_n))_n$ is uniformly distributed modulo 1. As a consequence, $(a^n)_n$ is Benford in base b if and only if $\log_b a$ is irrational.

Since $\log_b\left(\frac{k}{k-1}\right)$ decreases as k increases, the Benford sequences satisfy the so called *first digit phenomenon*: the terms with small first digit k are more frequent than the others. For example, for large n, the frequency of numbers with first digit 1 in base 10 among $2, 4, \dots, 2^n$ is approximately 30.1 percent. Among other fast growing sequences of positive numbers [13], the sequences $(n!)_n$, $(\prod_1^n p_k)_n$ and $(n^n)_n$ are Benford in any base b. Moreover $(n)_n$ and $(p_n)_n$ satisfy somehow the first digit phenomenon but in a weaker sense only [7].

The sequence $(\{\alpha p_n\})_n$ is uniformly distributed modulo 1 when α is irrational [21, pp. 105–107]. This and simple calculations prove that the sequence of Mersenne numbers $(2^{p_n} - 1)_n$ is Benford in base b whenever b is not a power of 2. Some computer simulations we have made suggest that the law of the random variable

$\mathcal{M}_{10}(p_n^*)$ does not converge weakly as $n \to +\infty$ whereas, as proved below, the law of $\mathcal{M}_b((2^{p_n^*} - 1))_n$ converges weakly to B_b whenever b is not a power of 2.

In many cases, the law of the mantissa in base b of products of independent or stationary positive random variables converges weakly to B_b [4].

1.5 Information about $\eta(\alpha)$

Roth and Baker received the Fields Medal in 1958 and 1970 respectively for their contributions on this subject. The terms *irrationality exponent*, *measure of irrationality* and *approximation exponent* also designate $\eta(\alpha)$ (see Section 1.1) or $\eta(\alpha) + 1$ in the literature. The Liouville numbers [17, p. 310] are the reals of infinite type; they are very well approximated by rationals. By Roth Theorem, all the algebraic numbers are of type 1 [3, p. 169]; they are badly approximated by rationals. Here is what is known, excepting possible recent improvements, on the type of some common transcendental numbers:

$$\eta(e) = 1\,,\ \eta(\pi) < 6.2\,,\ \eta(\pi^2) < 4.5\,,\ \eta(\log 2) < 2.6 \ \text{ and } \ \eta(\log 3) < 4.2.$$

(we have rounded to one decimal place for simplicity). See [23] for references.

The set $\{\alpha : \eta(\alpha) > 1\}$ has Lebesgue measure zero [3, p. 168] but is uncountable since each real greater than 1 is the type of at least one transcendental non-Liouville number [19, Corollary 4.].

All the quadratic numbers are of constant type (see Section 1.1) according to Liouville's theorem [17, p. 299]. The number e is not of constant type although $\eta(e) = 1$ [17, p. 294]. So the quadratic irrationals are more badly approximated by rationals than e.

2 Results and comments

We collect here the statements of our main results and compare them with existing literature.

2.1 Limit law of $\{\alpha Y_n\}$ and $\mathcal{M}_b(a^{Y_n})$

Note that the values of $\{\alpha Y_n\}$ are concentrated in a finite subset of $[0, 1)$ when α is rational and so the law of $\{\alpha Y_n\}$ cannot converge to U in this case. Recall that $\kappa(n) = q_1 + \cdots + q_n$.

Theorem 1. *The law of the random variable $\{\alpha Y_n\}$ converges weakly to U as $n \to +\infty$ whenever α is irrational, $(q_n)_n$ decreases to 0 and $\lim_n \kappa(n) = +\infty$.*

The treatment of the mantissa of a^{Y_n} derives easily from the above theorem. It may be worth reminding the reader that there exists no positive random variable Z such that $\mathcal{M}_b(Z)$ is distributed following B_b for every numeration base b [4, Proposition 5.2].

Corollary 1. *Suppose that $(q_n)_n$ decreases to 0 and that $\lim_n \kappa(n) = +\infty$. Then the law of $\mathcal{M}_b(a^{Y_n})$ converges weakly to B_b as $n \to +\infty$ whenever $\log_b a$ is irrational. Moreover the law of $\mathcal{M}_b(2^{Y_n} - 1)$ converges weakly to B_b whenever b is not a power of 2.*

2.2 Rates of convergence

Let Q_n and Q_n^* designate the law of $\{\alpha Y_n\}$ and that of $\mathcal{M}_b(a^{Y_n})$ respectively. We are now concerned with the Kolmogorov-Smirnov distance between Q_n and U,

$$\Delta(Q_n, U) = \sup_{0 \le s < 1} |Q_n([0, s)) - s|,$$

and in

$$\Delta(Q_n^*, B_b) = \sup_{1 \le t < b} |Q_n^*([1, t)) - \log_b t|.$$

Note that

$$\Delta(Q_n, U) = \Delta(Q_n^*, B_b) \tag{2}$$

if $\alpha = \log_b a$ (replace $\log_b t$ by s in (1)).

Because of the factor $|\sin(\pi h \alpha)|^{-1}$ in (8) (see Section 4.2), we need to know to what extent the values of $\langle h\alpha \rangle$ are close to zero as $h \to +\infty$. This is why our bounds depend on $\eta(\alpha)$. Recall that $\lambda(n) = q_n/\sqrt{\kappa(n-1)}$. Here are a few examples of asymptotics of $\lambda(n)$: $\lambda(n) \sim (\log n)^{-\frac{1}{2}} n^{-1}$ when $q_n = n^{-1}$, $\lambda(n) \sim 2^{-\frac{1}{2}} n^{-\frac{3}{4}}$ when $q_n = n^{-\frac{1}{2}}$ and $\lambda(n) \sim (\log n)^{-\frac{1}{2}} n^{-\frac{1}{2}}$ when $q_n = (\log n)^{-1}$.

Theorem 2. *Suppose that α is an irrational of finite type (see Sections and 1.1 and 1.5) and that the q_n decrease to 0 and sum to infinity. Denote by $\eta(\alpha)$ the type of α. Then*

$$\Delta(Q_n, U) = \mathcal{O}\left(\lambda(n)^{\frac{1}{\eta}}\right)$$

for all $\eta > \eta(\alpha)$.

In particular $\Delta(Q_n, U) = \mathcal{O}\left(\lambda(n)^{\frac{1}{\eta}}\right)$ for all $\eta > 1$ when α is algebraic or equal to e and $\Delta(Q_n, U) = \mathcal{O}\left(\lambda(n)^{\frac{1}{6.2}}\right)$ when $\alpha = \pi$.

By way of comparison, $\Delta(U_{\alpha,n}, U) = \mathcal{O}\left((1/n)^{\frac{1}{\eta}}\right)$ for all $\eta > \eta(\alpha)$ if $U_{\alpha,n}$ designates the uniform probability measure on the set $\{\{\alpha k\} : k = 1, \ldots, n\}$ [11, p. 123]. Moreover $\Delta(Q_n^{\pm\alpha}, U) = \mathcal{O}\left((1/\sqrt{n})^{\frac{1}{\eta}}\right)$ for all $\eta > \eta(2\alpha)$ if $Q_n^{\pm\alpha}$ designates the law of $\{\alpha Z_n\}$ and Z_n is the sum of n independent and identically distributed random variables taking values -1 and 1 with probabilities 1/2 [20, Theorem 5.5] and $\Delta(Q_n, U) = \mathcal{O}(1/\sqrt{n})$ if Q_n designates the law of $\{\alpha Z_n\}$ and Z_n is the sum of n independent and identically distributed integer valued random variables with finite variance and α is of contant type [2, Theorem 1.1] .

Again the treatment of the mantissa of a^{Y_n} derives easily from the above theorem.

Corollary 2. *Suppose that $\log_b a$ is irrational and that the q_n decrease to 0 and sum to $+\infty$. Let F denotes the set of prime factors of b. Then*

$$\Delta(Q_n^*, B_b) = \mathcal{O}\left(\lambda(n)^{\frac{1}{\eta}}\right)$$

, where we can choose $\eta = 2.5 \cdot 10^4 \log a \log b$ in the general case and, when $a = 2$, $\eta = 7.7$ if $F = \{2, 3\}$, $\eta = 15.3$ if $F = \{2, 3, 5\}$ and $\eta = 256.9$ if $F = \{2, 3, 5, 7\}$.

Several other particular values of a can be discussed in view of Lemma 5 and of the arguments featuring in the proof of Proposition 1.

Now we set $q_n = (\log n)^{-1}$. In this case, $Y_n = p_n^*$, the nth-Cramér number, and $2^{Y_n} - 1$ is the n-th Mersenne-Cramér number.

Corollary 3. *The conclusions of Corollary 2 remain true (with $\lambda(n) \sim (n \log n)^{-\frac{1}{2}}$) when Q_n^* denotes the law of $\mathcal{M}_b(2^{p_n^*} - 1)$.*

In particular, when Q_n^* denotes the law of the mantissa in base 10 of the nth Mersenne-Cramér number,

$$\Delta(Q_n^*, B_{10}) = \mathcal{O}\left((n \log n)^{-\frac{1}{30.6}}\right).$$

We can slightly improve the bound in Theorem 2 when α is an irrational quadratic number, like $\sqrt{2}$ or the golden ratio, or more generally when it is of constant type (see Sections and 1.1 and 1.5).

Theorem 3. *Suppose that α is an irrational of constant type and that the q_n decrease to 0 and sum to infinity. Then*

$$\Delta(Q_n, U) = \mathcal{O}\left(\lambda(n) \log^2(1/\lambda(n))\right).$$

In particular,

$$\Delta(Q_n, U) = \mathcal{O}\left(n^{-1} \log^{\frac{3}{2}} n\right)$$

if $q_n = 1/n$ and

$$\Delta(Q_n, U) = \mathcal{O}\left((n^{-1}(\log\log n)^{-\frac{1}{2}} \log n\right)$$

if $q_n = 1/(n \log n)$.

On the other hand, let $(x_n)_n$ be any sequence in $[0, 1)$ and $Q_n^{(x)}$ designate the uniform probability measure on the set $\{x_k : k = 1, \ldots, n\}$ $(n = 1, 2, \ldots)$. Then $\Delta(Q_n^{(x)}, U) = \mathcal{O}\left(n^{-1} \log n\right)$ when $x_n = \{\alpha n\}$ and α is any irrational quadratic number [11, p. 125] and when $(x_n)_n$ is the van der Corput sequence [11, p. 127] frequently used to approximate integrals by quasi-Monte Carlo methods. No smaller order of magnitude of $\Delta(Q_n^{(x)}, U)$ is possible [11, p. 109].

So the convergence rate of Q_n when α is a quadratic irrational and $q_n = 1/(n \log n)$ is better than the best possible convergence rate of $Q_n^{(x)}$. And it is even slightly better if we choose $q_n = 1/(n \log n \log\log n)$ and so on. However, we must take into account, that for each fixed n, the set of atoms of $Q_n^{(x)}$ is finite, while that of Q_n is not.

3 Preliminaries

We present here the main tools used in the following.

3.1 Weak convergence on the circle $[0, 1)$

The Lévy continuity theorem states that the weak convergence of a sequence of probability measures on the real line is characterized by the pointwise convergence of the corresponding characteristic functions. For probability measures on the circle $[0, 1)$, the convergence of the Fourier coefficients suffices. We present here the case where the limit distribution is U. Let $Z, Z_1, Z_2, \ldots$ be some random variables taking their values in $[0, 1)$.

Lemma 1 is the Weyl criterion. A direct proof is easily obtained by extending the arguments in [11, p. 7] to general sequences of probability measures. It is also a consequence of Lemma 2 below which has been established later.

Lemma 1. *In order that the law of Z_n converges weakly to U as $n \to +\infty$ it is necessary and sufficient that, for every positive integer h,*

$$\lim_{n\to+\infty} \mathbb{E}(e_h(Z_n)) = 0.$$

Lemma 2 is the Erdős-Turán inequality. It is a kind of Berry-Esseen theorem on the circle [14]. Theorem 1 in [14] is the most general version in the univariate case. Here is a simplified formulation which is sufficient in our network.

Lemma 2. *Let Q stand for the law of Z. Then, for every positive integer H,*

$$\sup_{0\le t<1} |Q([0,t)) - t| \le C\left(\frac{1}{H} + \sum_{h=1}^{H} \frac{|\mathbb{E}(e_h(Z))|}{h}\right),$$

where the constant C is independent of H.

3.2 Concentration function

We will make use of general results on the Lévy concentration function [15, p. 38] to get some information about the maximal size of the atoms of S_n. Lemma 3 derives from Lemma 1 in [15, p. 38] because, when $n_1 \le n_2$, S_{n_1} and $S_{n_2} - S_{n_1}$ are independent.

Lemma 3. *If $n_1 \le n_2$, then*

$$\max_{0\le j\le n_1} P(S_{n_1} = j) \ge \max_{0\le j\le n_2} P(S_{n_2} = j).$$

Lemma 4 is a particular case of the Kolmogorov-Rogozin inequality on concentration function (Theorem 4 in [15, p. 44]).

Lemma 4. *When $(q_n)_n$ decreases to 0,*

$$\max_{0\le j\le n} P(S_n = j) = \mathcal{O}\left(\kappa(n)^{-\frac{1}{2}}\right),$$

where $\mathcal{O}$ denotes the Landau big O.

3.3 The type of $\log_b a$

Let a and b be two integers both greater than 1. We need some upper bounds for $\eta(\log_b a)$ to investigate the rate of convergence of the law of $\mathcal{M}_b(a^{Y_n})$. Recall that $[y]$ denotes the nearest integer value of y. If we find $c > 0$ and $\gamma_0 > 0$ such that

$$|h\alpha - [h\alpha]| \ge ch^{-\gamma_0} \text{ for all sufficiently large } h, \tag{3}$$

then we show that $\eta(\alpha) \le \gamma_0$. If $\alpha = \log_b a$, then

$$|h\alpha - [h\alpha]| = (\log b)^{-1}|h\log a - k\log b|,$$

where $k = [h\log_b a]$. So lower bounds on linear forms in logarithms can yield upper bounds on measure of irrationality.

According to the Gelfond-Schneider theorem [3, p. 2], $\log_b a$ cannot be an irrational algebraic number. It is either rational (when a is a rational power of b) or transcendental. According to Baker's Theorem [3, p. 2] it is of finite type. However Baker's initial papers provide general upper bounds of $\eta(\log_b a)$ which are far too large to be meaningful in our context. In [10], the authors derive from them that $\eta(\log_{10} 2) \leq 2.4 \cdot 10^{602}$. Improving Baker's general bounds has motivated many authors including Baker himself. See [3, pp. 195–221] for references.

It seems that the best available general result which can be helpful for us is Gouillon's one [9, Corollary 2.3.] which leads to

$$\eta(\log_b a) < 4 \cdot 10^4 \log a \log b. \tag{4}$$

Some results of Rhin [16] and of Wu [22] provide reasonable bounds of $\eta(\log_b a)$ when the prime factors of a and b are small and $\log_b a$ is irrational. The following lemma groups them in simplified versions and, aiming at simplicity and the investigation of the Mersenne-Cramér sequence, we then focus on the case $a = 2$.

Lemma 5. *Let u_1, u_2, u_3 and u_4 be four integers. Set $H_2 = \max(|u_1|, |u_2|)$, $H_3 = \max(|u_1|, |u_2|, |u_3|)$ and $H_4 = \max(|u_1|, |u_2|, |u_3|, |u_4|)$. Then, for sufficient large H_2, H_3 and H_4,*

$$|u_1 \log 2 + u_2 \log 3| \geq H_2^{-7.62},$$

$$|u_1 \log 2 + u_2 \log 3 + u_3 \log 5| \geq H_3^{-15.28},$$

$$|u_1 \log 2 + u_2 \log 3 + u_3 \log 5 + u_4 \log 7| \geq H_4^{-256.87}.$$

The following proposition may sound obvious to the specialists in view of Lemma 5, but they are not formulated in the papers of Rhin and Wu or anywhere else it seems.

Proposition 1. *Suppose that b is not a power of 2 and let F denotes the set of prime factors of b. Then $\eta(\log_b 2) \leq 7.62$ when $F \subset \{2, 3\}$, $\eta(\log_b 2) \leq 15.28$ when $F \subset \{2, 3, 5\}$ and $\eta(\log_b 2) \leq 256.87$ when $F \subset \{2, 3, 5, 7\}$.*

Proof. We only demonstrate the first statement. The proofs of the two others follow the same lines. Recall that $[x]$ stands for the nearest integer of x.

Suppose that $b = 2^{v_1} 3^{v_2}$ with $v_2 > 0$. For each positive integer h, set

$$k = [h\eta(\log_b 2)] \quad \text{and} \quad H = \max(|h - kv_1|, kv_2).$$

Lemma 5 ensures the existence of H_0 such that

$$|h \log_b 2 - k| = (\log b)^{-1} |(h - kv_1) \log 2 - kv_2 \log 3| \geq (\log b)^{-1} H^{-7.62}$$

for all $H \geq H_0$. Moreover $h\eta(\log_b 2) - 1 \leq k \leq h\eta(\log_b 2) + 1$ and so

$$(h\eta(\log_b 2) - 1)v_2 \leq kv_2 \leq H \leq h + kv_1 + kv_2 \leq Ch,$$

where $C = (1 + (\eta(\log_b 2) + 1)(v_1 + v_2))$. Then $H \geq H_0$ for sufficiently large h and this implies

$$|h \log_b 2 - k| \geq (\log b)^{-1} H^{-7.62} \geq (\log b)^{-1} C^{-7.62} h^{-7.62}.$$

This and (3) complete the proof. $\square$

4 Proofs

4.1 An important auxiliary result

We begin with a general property on Bernoulli trials whose proof uses and details some arguments of the proof of [12, Theorem 4.6.]. Recall the notation presented in Section 1.1.

Proposition 2. *For each fixed $n \geq 1$, the sequence $(P(S_m = n))_{m \geq n}$ is bell-shaped and*

$$\sum_{m=n}^{+\infty} |P(S_{m+1} = n) - P(S_m = n)| \leq 2 \max_{0 \leq j \leq n} P(S_n = j).$$

Proof. Fix $n \geq 1$. Then, for all $m \geq n$,

$$P(S_{m+1} = n) = q_{m+1} P(S_m = n-1) + (1 - q_{m+1}) P(S_m = n)$$

and this leads to

$$P(S_{m+1} = n) - P(S_m = n) = q_{m+1} \left(P(S_m = n-1) - P(S_m = n) \right). \tag{5}$$

By [6], the laws of the random variables S_m are bell-shaped and, when $\{\kappa(m)\}$ grows from 0 to 1, the mode is firstly at $\lfloor \kappa(m) \rfloor$, then at both $\lfloor \kappa(m) \rfloor$ and $\lfloor \kappa(m) \rfloor + 1$ and finally at $\lfloor \kappa(m) \rfloor + 1$.

Hence, as m grows, $P(S_m = n-1) - P(S_m = n)$ is

- nonnegative when $\kappa(m) < n - 1$,
- nonnegative when $n - 1 \leq \kappa(m) \leq n$ and the mode is at $\lfloor \kappa(m) \rfloor$,
- nul when $n - 1 \leq \kappa(m) \leq n$ and the mode is at both $\lfloor \kappa(m) \rfloor$ and $\lfloor \kappa(m) \rfloor + 1$,
- nonpositive when $n - 1 \leq \kappa(m) \leq n$ and the mode is at $\lfloor \kappa(m) \rfloor + 1$,
- nonpositive when $n < \kappa(m)$.

The same applies for $P(S_{m+1} = n) - P(S_m = n)$ in view of (5) and so the sequence $(P(S_m = n))_{m \geq n}$ is bell-shaped. This yields

$$\sum_{m=n}^{+\infty} |P(S_{m+1} = n) - P(S_m = n)| \leq 2 \max_{0 \leq j \leq m_0} P(S_{m_0} = j)$$

for some $m_0 \geq n$. According to Lemma 3,

$$\max_{0 \leq j \leq m_0} P(S_{m_0} = j) \leq \max_{0 \leq j \leq n} P(S_n = j).$$

The proof is completed. $\square$

4.2 Proof of Theorem 1

Let α be any irrational. By Lemma 1 we need only to check that, for all positive integers h,

$$\lim_{n\to+\infty}\mathbb{E}(e_h(\alpha Y_n)) = \lim_{n\to+\infty}\sum_{m=n}^{+\infty} P(Y_n = m)e_h(\alpha m) = 0.$$

The random variables X_n being independent,

$$P(Y_n = m) = q_m P(S_{m-1} = n-1) \tag{6}$$

for all $m \geq n$. Fix the positive integers n, h and $N \geq n$ and set $\sigma_m = \sum_{j=n}^{m} q_j e_h(\alpha j))$.

When α is irrational, $|\sum_{l=k}^{K} e_h(\alpha l)| \leq |\sin(\pi h\alpha)|^{-1}$ for all positive integers k and K with $k < K$. Hence a summation by parts gives for every $m \geq n$

$$\begin{aligned}|\sigma_m| &= \left|q_m \sum_{j=n}^{m} e_h(\alpha j) + \sum_{j=n}^{m-1}(q_j - q_{j+1})\sum_{l=n}^{j} e_h(\alpha l)\right| \\ &\leq \left(q_m + \sum_{j=n}^{m-1}(q_j - q_{j+1})\right)|\sin(\pi h\alpha)|^{-1} = q_n|\sin(\pi h\alpha)|^{-1}\end{aligned} \tag{7}$$

(recall that $(q_n)_n$ is decreasing). By (6) and another summation by parts, we get

$$\begin{aligned}\sum_{m=n}^{N} P(Y_n = m)e_h(\alpha m) =& \sum_{m=n}^{N} P(S_{m-1} = n-1)q_m e_h(\alpha m) \\ =& P(S_{N-1} = n-1)\sigma_N \\ &+ \sum_{m=n}^{N-1}(P(S_{m-1} = n-1) - P(S_m = n-1))\sigma_m.\end{aligned}$$

Then Lemma 3, Proposition 2 and (7) yield for every $N \geq n$

$$\begin{aligned}\left|\sum_{m=n}^{N} P(Y_n = m)e_h(\alpha m)\right| \leq& \frac{q_n}{|\sin(\pi h\alpha)|}\max_{0\leq j\leq N-1} P(S_{N-1} = j) \\ &+ \frac{2q_n}{|\sin(\pi h\alpha)|}\max_{0\leq j\leq n-1} P(S_{n-1} = j) \\ \leq& \frac{3q_n}{|\sin(\pi h\alpha)|}\max_{0\leq j\leq n-1} P(S_{n-1} = j).\end{aligned}$$

We have demonstrated that

$$|\mathbb{E}(e_h(\alpha Y_n))| \leq \frac{3q_n}{|\sin(\pi h\alpha)|}\max_{0\leq j\leq n-1} P(S_{n-1} = j) \tag{8}$$

which concludes our proof because $\lim_n q_n = 0$ (see also Lemma 4).

4.3 Proof of Corollary 1

The first assertion is a direct consequence of Theorem 1 and Section 1.4.

Assume that b is not a power of 2 and that $q_n = (\log n)^{-1}$ for $n \geq 3$. Then $Y_n = p_n^*$ and so the law of $\{\log_b(2^{p_n^*})\}$ converges weakly to the U because $\log_b 2$ is irrational.

In view of Section 1.4 and Lemma 1, it remains only to check that, for all positive integers h,

$$\lim_{n\to+\infty} \mathbb{E}\big(e_h(\log_b(2^{p_n^*})) - e_h(\log_b(2^{p_n^*}-1))\big) = 0.$$

But

$$e_h(\log_b(2^{p_n^*})) - e_h(\log_b(2^{p_n^*}-1)) = e_h(\log_b(2^{p_n^*}))\left(1 - e_h(\log_b(1-2^{-p_n^*}))\right)$$

and so $(e_h(\log_b(2^{p_n^*})) - e_h(\log_b(2^{p_n^*}-1)))_n$ is a bounded sequence of random variables which converges almost surely to 0 as $n \to +\infty$ because $(p_n^*)_n$ converges almost surely to $+\infty$. The Lebesgue dominated convergence theorem completes the proof.

4.4 Proof of Theorem 2

Fix $\eta > \eta(\alpha)$. Using Lemma 2, we get for all positive integers H

$$\begin{aligned}\Delta(Q_n, U) &\leq C\left(\frac{1}{H} + \sum_{h=1}^{H} \frac{|\mathbb{E}(e_h(\alpha Y_n))|}{h}\right)\\ &\leq C\left(\frac{1}{H} + \mathcal{O}(\lambda(n))\sum_{h=1}^{H}\frac{1}{h|\sin(\pi h\alpha)|}\right),\end{aligned}$$

because, by (8) and Lemma 4,

$$|\mathbb{E}(e_h(\alpha Y_n))| = \frac{\mathcal{O}(\lambda(n))}{|\sin(\pi h\alpha)|}.$$

We have $|\sin(\pi h\alpha)| = \sin(\pi\langle h\alpha\rangle) \geq 2\langle h\alpha\rangle$ since $\langle h\alpha\rangle \leq 1/2$. Moreover $\langle h\alpha\rangle \geq h^{-\eta}$ for sufficiently large h by definition of $\eta(\alpha)$ (see Section 1.1). So direct calculations yield $\sum_{h=1}^{H}(h|\sin(\pi h\alpha)|)^{-1} = \mathcal{O}(H^\eta)$, but the particular nature of the sequence $(\langle h\alpha\rangle)_h$ provides a better estimate, namely

$$\sum_{h=1}^{H}\frac{1}{h|\sin(\pi h\alpha)|} = \mathcal{O}(H^{\eta-1}) \tag{9}$$

(see [11, p. 123]). We then arrive at

$$\Delta(Q_n, U) \leq C\left(\frac{1}{H} + \mathcal{O}(\lambda(n))\mathcal{O}(H^{\eta-1})\right). \tag{10}$$

We choose $H = \lfloor \lambda(n)^{-\frac{1}{\eta}} \rfloor$ and get

$$\Delta(Q_n, U) = \mathcal{O}\left(\lambda(n)^{\frac{1}{\eta}}\right).$$

The two others assertions derive from the first one and Section 1.5.

4.5 Proof of Corollaries 2 and 3

Recall that

$$\Delta(Q_n, U) = \Delta(Q_n^*, B_b) \tag{11}$$

if $\alpha = \log_b a$. So Corollary 2 is a consequence of Theorem 2 and of (4) and Proposition 2 in Section 3.3.

Classical arguments give

$$\begin{aligned} |e_h(\log_b(2^{p_n^*})) - e_h(\log_b(2^{p_n^*} - 1))| &= |e_h(\log_b(2^{p_n^*}))||(1 - e_h(\log_b(1 - 2^{-p_n^*}))| \\ &= \mathcal{O}(2^{-p_n^*}) = \mathcal{O}(2^{-n}) \end{aligned}$$

since $p_n^* \geq n$. Hence

$$|\mathbb{E}(e_h(\log_b(2^{p_n^*} - 1)))| = |\mathbb{E}(e_h(\log_b(2^{p_n^*})))| + \mathcal{O}(2^{-n}).$$

In view of (9) this implies

$$\begin{aligned} \sum_{h=1}^{H} \frac{|\mathbb{E}(e_h(\log_b(2^{p_n^*} - 1)))|}{h} &= \mathcal{O}(\lambda(n))\mathcal{O}(H^{\eta-1}) + \mathcal{O}(2^{-n})\mathcal{O}(\log H) \\ &= \mathcal{O}(\lambda(n))\mathcal{O}(H^{\eta-1}) \end{aligned}$$

for all $\eta > \eta(\log_b 2)$. So the final arguments of the proof of Theorem 2 apply again and this proves Corollary 3.

4.6 Proof of Theorem 3

Suppose that α is of contant type. Then $\eta(\alpha) = 1$ and $h\langle h\alpha\rangle > c$ for all positive integers h and some $c > 0$ independent of h (see Section 1.1). In this case $\sum_{h=1}^{H}(h|\sin(\pi h\alpha)|)^{-1} = \mathcal{O}(\log^2 H)$ according to Lemma 3.3 in [11, p. 123] (here $\log^2 x$ means $(\log x)^2$). Moreover, we no longer need to consider $\eta > \eta(\alpha)$ in the proof of Theorem 2.

So we can replace η by 1 and $\mathcal{O}(H^{\eta-1})$ by $\mathcal{O}(\log^2 H)$ in (9) and (10) and get

$$\Delta(Q_n, U) = \mathcal{O}\left(\lambda(n)\log^2(1/\lambda(n))\right).$$

The two other assertions derive from the first one and simple calculations.

5 Concluding remark

We are unable to provide general and meaningful lower bounds for $\Delta(Q_n, U)$. However what follows makes us hope that the estimates featuring in Theorem 2 are quite accurate.

We have supposed for simplicity that q_n decreases to 0 but our arguments still apply when all the q_n are equal to $q > 0$ (with minor changes in Lemma 4 and its consequences when $q > 1/2$). In this case Y_n is the sum of n independent and identically distributed random variables distributed following the geometric distribution with parameter q. These random variables being square integrable, [8, Theorem 4.2] leads to

$$\sup_{m \geq n} P(Y_n = m) \geq C_1 n^{-\frac{1}{2}}$$

for some constant $C_1 > 0$. The maximal size of the atoms of the law of $\{\alpha Y_n\}$ admits the same lower bound. Therefore

$$2\Delta(Q_n, U) \geq C_1 n^{-\frac{1}{2}}$$

whatever is the value of $\eta(\alpha)$. On the other hand, when all the q_n are equal to $q > 0$, $\lambda(n) = \frac{\sqrt{q}}{\sqrt{n-1}}$ and so, if in addition α is quadratic irrational, Theorem 3 gives

$$\Delta(Q_n, U) \leq C_2 n^{-\frac{1}{2}} (\log n)^2$$

for some $C_2 > 0$.

References

[1] Berger A. and Hill T.P. (2011), *A basic theory of Benford's Law*, Probab. Surv., 8, 1–126.

[2] Berkes I. and Borda B. (2018), *Berry-Esseen bounds and Diophantine approximation*, Anal. Math., 44, 149–161.

[3] Bugeaud Y. (2018), *Linear Forms in Logarithms and applications*, IRMA Lect. Math. Theor. Phys. 28, Eur. Math. Soc., Zürich.

[4] Chenavier N., Massé B. and Schneider D. (2018), *Products of random variables and the first digit phenomenon*, Stoch. Process. Appl., 128, 1615–1634.

[5] Cramér H. (1935), *Prime numbers and probabilities*, Skand. Math. Kongr., 8, 107–115.

[6] Darroch J. N. (1964), *On the distribution of successes in independent trials*, Ann. Math. Stat., 35-3, 1317–1321.

[7] S. Eliahou, B. Massé, and D. Schneider, *On the mantissa distribution of powers of natural and prime numbers*, Acta. Math. Hungar. 139-1-2 (2013), 49–63.

[8] Esseen C. G. (1968), *On the concentration function of a sum of independent random variables*, Z. Wahrscheinlichkeitstheor. verw. Geb., 9, 290–308.

[9] Gouillon N. (2006), *Explicit lower bounds for linear forms in two logarithms*, J. Théor. Nr. Bordx, 18, 127–146.

[10] Kontorovich A.V. and Miller S.J. (2005), *Benford's Law, Values of L-functions and the* $3x + 1$ *problem*, Acta Arith.,120, 269–297.

[11] Kuipers L. and Niederreiter H. (2006), *Uniform Distribution of Sequences*, Dover Publications New-York.

[12] Massé B. and Schneider D. (2012), *Random number sequences and the first digit phenomenon*, Electron. J. Probab., 17, 1–17.

[13] Massé B. and Schneider D. (2015), *Fast growing sequences of numbers and the first digit phenomenon*, Int. J. Number Theory, 11-3, 705–719.

[14] Niederreiter H. and Philipp W. (1973), *Berry-Esseen bounds and a theorem of Erdős and Turán on uniform distribution mod 1*, Duke Math. J., 40, 633–649.

[15] Petrov V. (1975), *Sums of Independent Random Variables*, Springer-Verlag.

[16] Rhin G. (1987), *Approximants de Padé et mesures effectives d'irrationalité*, Prog. Math., 71-1, 155–164.

[17] Ribenboim P. (2000), *My Numbers, My Friends : Popular Lectures on Number Theory*, Springer-Verlag.

[18] Ribenboim P. (2004), *The Little Book of Bigger Primes*, Springer.

[19] Sondow J. (2004), *Irrationality measures, irrationality bases, and a theorem of Jarnik*, arXiv:math/0406300.

[20] Su F. E. (1998), *Convergence of random walks on the circle generated by an irrational rotation*, Trans. Amer. Math. Soc., 350-9, 3717–3741.

[21] Tenenbaum G. and Mendès France M. (2011), *Les nombres premiers entre l'ordre et le chaos*, Dunod Paris.

[22] Wu Q. (2003), *On the linear independence measure of logarithms of rational numbers*, Math. Comput., 72-242, 901–911.

[23] https://mathworld.wolfram.com/IrrationalityMeasure.html

[24] https://mersenne.org/primes/