On the construction of absolutely normal numbers

Christoph Aistleitner
Institute of Analysis and Number Theory
Graz University of Technology
A-8010 Graz, Austria
E-mail: aistleitner@math.tugraz.at

Verónica Becher
Departamento de Computación, Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires & ICC, CONICET
Pabellón I, Ciudad Universitaria, C1428EGA Buenos Aires, Argentina
E-mail: vbecher@dc.uba.ar

Adrian-Maria Scheerer
Institute of Analysis and Number Theory
Graz University of Technology
A-8010 Graz, Austria
E-mail: scheerer@math.tugraz.at

Theodore A. Slaman
Department of Mathematics
University of California Berkeley
719 Evans Hall #3840, Berkeley, CA 94720-3840 USA
E-mail: slaman@math.berkeley.edu

July 8, 2017

Abstract

We give a construction of an absolutely normal real number x such that for every integer b greater than or equal to 2, the discrepancy of the first N terms of the sequence $(b^n x \mod 1)_{n \geq 0}$ is of asymptotic order $\mathcal{O}(N^{-1/2})$. This is below the order of discrepancy which holds for almost all real numbers. Even the existence of absolutely normal numbers having a discrepancy of such a small asymptotic order was not known before.

1   Introduction and statement of results

For a sequence $(x_j)_{j\geq 0}$ of real numbers in the unit interval, the discrepancy of the first N elements is

$$D_N((x_j)_{j\geq 0}) = \sup_{0\leq\alpha_1<\alpha_2\leq 1} \left| \frac{1}{N}\#\{j : 0 \leq j \leq N-1 \text{ and } \alpha_1 \leq x_j < \alpha_2\} - (\alpha_2 - \alpha_1) \right|.$$

A sequence $(x_j)_{j\geq 0}$ of real numbers in the unit interval is uniformly distributed if and only if $\lim_{N\to\infty} D_N((x_j)_{j\geq 0}) = 0$.

The property of Borel normality can be defined in terms of uniform distribution. For a real number x, we write $\{x\} = x - \lfloor x \rfloor$ to denote the fractional part of x. A real number x is normal with respect to an integer base b greater than or equal to 2 if the sequence $(\{b^j x\})_{j\geq 0}$ is uniformly distributed in the unit interval. The numbers which are normal to all integer bases are called absolutely normal. In this paper we prove the following theorem.

Theorem 1. *There is an absolutely normal number x such that for each integer $b \geq 2$, there are numbers $N_0(b)$ and C_b such that for all $N \geq N_0(b)$,*

$$D_N((\{b^j x\})_{j\geq 0}) \leq \frac{C_b}{\sqrt{N}}.$$

For the constant C_b we can choose $C_b = 3433 \cdot b$. Moreover, there is an algorithm that computes the first N digits of the expansion of x in base 2 after performing exponential in N mathematical operations.

It follows from the work of Gál and Gál [6] that for almost all real numbers (in the sense of Lebesgue measure) and for all integer bases b greater than or equal to 2 the discrepancy of the sequence $(\{b^j x\})_{j\geq 0}$ obeys the law of iterated logarithm. Philipp [10] gave explicit constants and Fukuyama [5, Corollary]) sharpened the result. He proved that for every real $\theta > 1$ there is a constant C_θ such that for almost all real x we have

$$\limsup_{N\to\infty} \frac{\sqrt{N}D_N((\{\theta^j x\})_{j\geq 0})}{\sqrt{\log\log N}} = C_\theta.$$

In case θ is an integer greater than or equal to 2, for C_θ one has the values

$$C_\theta = \begin{cases} \sqrt{84}/9, & \text{if } \theta = 2, \\ \sqrt{(\theta+1)/(\theta-1)}/\sqrt{2}, & \text{if } \theta \text{ is odd}, \\ \sqrt{(\theta+1)\theta(\theta-2)/(\theta-1)^3}/\sqrt{2}, & \text{if } \theta \geq 4 \text{ is even}. \end{cases}$$

To prove Theorem 1 we give a construction of a real number x such that, for every integer b greater than or equal to 2, $D_N((\{b^j x\})_{j\geq 0})$ is of asymptotic order $\mathcal{O}(N^{-1/2})$, hence, below the order of discrepancy that holds for almost all real numbers. The existence

of absolutely normal numbers having a discrepancy of such a small asymptotic order was not known before.

To prove Theorem 1, we define a computable sequence of nested binary intervals $(\Omega_k)_{k \geq 1}$ such that for all elements of Ω_k the discrepancy $D_N((\{b^j x\})_{j \geq 0})$ is sufficiently small for some range of b and N. This argument uses methods going back to Gál and Gál [6] and Philipp [10]. The unique point in the intersection $\bigcap_{k \geq 1} \Omega_k$ is a computable number which satisfies the discrepancy estimate in the conclusion of the theorem. This is the number we obtain. The construction uses just discrete mathematics and yields directly the binary expansion of the computed number. Unfortunately, the algorithm that computes the first N digits performs exponential in N many operations.

In view of the method used to prove Theorem 1, the appearance of a bound of square-root order for the discrepancy is very natural. Note that the discrepancy is exactly the same as the Kolmogorov–Smironov statistic, applied to the case of the uniform distribution on $[0, 1]$. By Kolmogorov's limit theorem the Kolmogorov–Smirnov statistic of a system of independent, identically distributed (i.i.d.) random variables has a limit distribution when normalized by $\sqrt{N}$ (somewhat similar to the case of the central limit theorem). Since it is well-known that so-called lacunary function systems (such as the system $(\{b^j x\})_{j \geq 0}$ for $b \geq 2$) exhibit properties which are very similar to those of independent random systems, we can expect a similar behavior for the discrepancy of $(\{b^j x\})_{j \geq 0}$. In other words, we can find a set of values of x which has positive measure, and whose discrepancy is below some appropriate constant times the square-root normalizing factor (see [1] for more details). Since the sequence $(b^j)_{j \geq 0}$ is very quickly increasing, we can iterate this argument and find a "good" set of values of x (which we call Ω_k) which gives the desired discrepancy bound and which has positive measure *within* the previously constructed set Ω_{k-1}. These remarks show why a discrepancy bound of order $N^{-1/2}$ is a kind of barrier when constructing the absolutely normal number x using probabilistic methods. Accordingly, any further improvement of Theorem 1 would require some truly novel ideas.

As reported in [11], prior to the present work the construction of an absolutely normal number with the smallest discrepancy bound was due to Levin [8]. Given a countable set L of reals greater than 1, Levin constructs a real number x such that for every θ in L,

$$D_N((\{\theta^j x\})_{j \geq 0}) < \frac{C_\theta (\log N)^3}{\sqrt{N}},$$

for a constant C_θ for every $N \geq N_0(\theta)$. His construction does not produce directly the binary expansion of the defined number x. Instead it produces a computable sequence of real numbers that converge to x and the computation of the N-th term requires double-exponential (in N) many operations including trigonometric operations, see [2].

It is possible to prove a version of Theorem 1 replacing the set of integer bases by any subset of computable reals greater than 1. The proof would remain essentially the same except for a suitable version of Lemma 3. In contrast, we do not know if it is possible obtain a version of Theorem 1 where the exponential computational complexity is replaced with polynomial computational complexity as in [3].

Theorem 1 does not supersede the discrepancy bound obtained by Levin [9] for the discrepancy of a normal number with respect to one fixed base. For a fixed integer $b \geq 2$, Levin constructed a real number x such that

$$D_N(\{b^j x\}_{j \geq 0}) < \frac{C_\theta (\log N)^2}{N}.$$

One should compare this upper bound with the lower bound obtained by Schmidt [12], who proved that there is a constant C for *every* sequence $(x_j)_{j \geq 0}$ of real numbers in the unit interval there are infinitely many Ns such that

$$D_N((x_j)_{j \geq 0}) > C \frac{\log N}{N}.$$

This lower bound is achieved by some so-called low-discrepancy sequences, (see [4] and the references there), but it remains an important open problem whether this optimal order of discrepancy can also be achieved by a sequence of the form $(\{b^j x\})_{j \geq 0}$ for a real number x.

Accordingly, two central questions in this field remain open:

- Asked by Korobov [7]: For a *fixed* integer $b \geq 2$, what is the function $\psi(N)$ with maximal speed of decrease to zero such that there is a real number x for which

  $$D_N(\{b^j x\}_{j \geq 0}) = \mathcal{O}(\psi(N)) \qquad \text{as } N \to \infty?$$

- Asked by Bugeaud (personal communication, 2017): Is there a number x satisfying the minimal discrepancy estimate for normality not only in one fixed base, but in all bases at the same time? More precisely, let ψ be Korobov's function from above. Is there a real number x such that for *all* integer bases $b \geq 2$,

  $$D_N(\{b^j x\}_{j \geq 0}) = \mathcal{O}(\psi(N)) \qquad \text{as } N \to \infty?$$

2   Definitions and lemmas

We use some tools from [6, 10]. For non-negative integers M and N, for a sequence of real numbers $(x_j)_{j \geq 0}$ and for real numbers α_1, α_2 such that $0 \leq \alpha_1 < \alpha_2 \leq 1$, we define

$$F(M, N, \alpha_1, \alpha_2, (x_j)_{j \geq 1}) = \left| \#\{j : M \leq j < M + N : \alpha_1 \leq x_j < \alpha_2\} - (\alpha_2 - \alpha_1)N \right|.$$

To shorten notations we will write $\{b^j x\}_{j \geq 0}$ to denote $(\{b^j x\})_{j \geq 0}$. Throughout the paper we will use the fact that

$$F\left(M, N, \alpha_1, \alpha_2, \{b^j x\}_{j \geq 0}\right) = F\left(0, N, \alpha_1, \alpha_2, \{b^{j+M} x\}_{j \geq 0}\right)$$

for every non-negative integer M.

The following lemma is a classical result from probability theory called Bernstein's inequality (see for example [14, Lemma 2.2.9]). We write μ for the Lebesgue measure and occasionally we write $\exp(x)$ for e^x.

Lemma 2. *Let* $X_1, \ldots, X_n$ *be i.i.d. random variables having zero mean and variance* σ^2, *and assume that their absolute value is at most 1. Then for every* $\varepsilon > 0$

$$\mathbb{P}\left(\left|\sum_{k=1}^{n} X_k\right| > \varepsilon\sqrt{n}\right) \leq 2\exp\left(\frac{-\varepsilon^2}{2\sigma^2 + 2/3\varepsilon n^{-1/2}}\right).$$

Lemma 3. *Let* $b \geq 2$ *be an integer, let* h *and* N *be positive integers such that* $N \geq h$, *and let* ε *be a positive real. Then for all integers* $M \geq 0$ *and* a *satisfying* $0 \leq a < b^h$,

$$\mu\left(\left\{x \in (0,1) : F\left(M, N, ab^{-h}, (a+1)b^{-h}, \{b^j x\}_{j \geq 0}\right) > \varepsilon\sqrt{hN}\right\}\right)$$

is at most

$$2h\exp\left(\frac{-\varepsilon^2}{2b^{-h}(1-b^{-h}) + 2/3\varepsilon\lfloor N/h\rfloor^{-1/2}}\right).$$

Proof of Lemma 3. We split the index set $\{M, M+1, \ldots, M+N-1\}$ into h classes, according to the remainder of an index when it is reduced modulo h. Then each of these classes contains either $\lfloor N/h \rfloor$ or $\lceil N/h \rceil$ elements. Let $\mathbf{1}_{[ab^{-h},(a+1)b^{-h})}(x)$ denote the indicator function of the interval $[ab^{-h}, (a+1)b^{-h})$. Let $\mathcal{M}_0$ denote the class of all indices in $\{M, \ldots, M+N-1\}$ which leave remainder zero when being reduced modulo h. Set $n_0 = \#\mathcal{M}_0$. Then it is an easy exercise to check that the system of functions $\left(\mathbf{1}_{[ab^{-h},(a+1)b^{-h})}(\{b^j x\}) - b^{-h}\right)_{j \in \mathcal{M}_0}$ is a system of i.i.d. random variables over the unit interval, equipped with Borel sets and Lebesgue measure.[1] The absolute value of these random variables is trivially bounded by 1, they have mean zero, and their variance is $b^{-h}(1-b^{-h})$. Thus by Lemma 2 we have

$$\mu\left(\left\{x \in (0,1) : \left|\sum_{j \in \mathcal{M}_0} \left(\mathbf{1}_{[ab^{-h},(a+1)b^{-h})}(\{b^j x\}) - b^{-h}\right)\right| > \varepsilon\sqrt{n_0}\right\}\right)$$

$$\leq 2\exp\left(\frac{-\varepsilon^2}{2b^{-h}(1-b^{-h}) + 2/3\varepsilon n_0^{-1/2}}\right).$$

Clearly similar estimates hold for the indices in the other residue classes. Let $n_1, \ldots, n_{h-1}$ denote the cardinalities of these other residue classes. By assumption $n_0 + \cdots + n_{h-1} = N$.

---

[1] These functions are Rademacher functions, just in base b^h instead of the usual base 2. See for example [13, Section 1.1.3] for more details.

Note that by the Cauchy-Schwarz inequality we have $\sqrt{n_0}+\cdots+\sqrt{n_{h-1}} \leq \sqrt{h}\sqrt{N}$. Thus, summing up, we obtain

$$\mu\left(\left\{x \in (0,1): \left|\left(\sum_{j=M}^{M+N-1} \mathbf{1}_{[ab^{-h},(a+1)b^{-h})}(\{b^j x\})\right) - Nb^{-h}\right| > \varepsilon\sqrt{hN}\right\}\right)$$

$$\leq\quad 2h\exp\left(\frac{-\varepsilon^2}{2b^{-h}(1-b^{-h})+2/3\varepsilon\lfloor N/h\rfloor^{-1/2}}\right).$$

This proves the lemma.   □

We will use a modified version of Lemma 3, which works on any subinterval A of $[0,1]$.

Lemma 4. *Let $b \geq 2$ be an integer, let h and N be positive integers such that $N \geq h$, and let ε be a positive real. Then for all integers $M \geq 0$ and a satisfying $0 \leq a < b^h$, for any subinterval A of $[0,1]$ and for any positive integer j_0,*

$$\mu\left(\left\{x \in A: F(M+j_0, N, ab^{-h}, (a+1)b^{-h}, \{b^j x\}_{j\geq 0}) > \varepsilon\sqrt{hN}\right\}\right)$$

is at most

$$2\mu(A)h\exp\left(\frac{-\varepsilon^2}{2b^{-h}(1-b^{-h})+2/3\varepsilon\lfloor N/h\rfloor^{-1/2}}\right)+2b^{-j_0}.$$

Proof of Lemma 4. Let B denote the largest interval contained in A which has the property that both of its endpoints are integer multiples of b^{-j_0}. Then $\mu(A\backslash B) \leq 2b^{-j_0}$. Furthermore, by periodicity we have

$$\mu\left(\{x \in B: F\left(M+j_0, N, ab^{-m}, (a+1)b^{-m}, \{b^j x\}_{j\geq 0}\right) > \varepsilon\sqrt{hN}\}\right)$$

$$=\quad \mu(B) \cdot \mu\left(\{x \in (0,1): F\left(M, N, ab^{-m}, (a+1)b^{-m}, \{b^j x\}_{j\geq 0}\right) > \varepsilon\sqrt{hN}\}\right),$$

for which we can apply the conclusion of Lemma 3. Note that $\mu(B) \leq \mu(A)$. This proves Lemma 4.   □

The following corollary follows easily from Lemma 4.

Corollary 5. *Let $b \geq 2$ be an integer, let h and N be positive integers such that $N \geq h$, and assume that ε satisfies*

(1) $$2/3\varepsilon\lfloor N/h\rfloor^{-1/2} \leq \frac{1}{bh^5}.$$

Then for all integers $M \geq 0$ and a satisfying $0 \leq a < b^h$, for any subinterval A of $[0,1]$ and for any positive integer j_0 we have

$$\mu\left(\left\{x \in A: F\left(M+j_0, N, ab^{-h}, (a+1)b^{-h}, \{b^j x\}_{j\geq 0}\right) > \varepsilon\sqrt{hN}\right\}\right)$$

is at most

$$\mu(A)2h\exp\left(\frac{-\varepsilon^2 bh^5}{529}\right)+2b^{-j_0}.$$

Proof. The corollary follows from Lemma 4 and the fact that

$$2b^{-h}(1 - b^{-h}) \leq 2b^{-h} \leq 528b^{-1}h^{-5}$$

for all $b \geq 2$ and $h \geq 1$ (for the second inequality in the displayed formula it is sufficient to check that $2^{-h+2} \leq 528h^{-5}$ for integers $h \geq 1$, which can be done numerically). Together with assumption (1) this implies that $2b^{-h}(1 - b^{-h}) + 2/3\varepsilon\lfloor N/h \rfloor^{-1/2} \leq 529b^{-1}h^{-5}$. $\square$

Remark 6. For any two reals α_1, α_2 such that $0 \leq \alpha_1 < \alpha_2 < 1$, and for any sequence $(x_j)_{j \geq 1}$ of reals, a trivial bound yields

$$F(0, N, \alpha_1, \alpha_2, (x_j)_{j \geq 1}) \leq 2 \sup_{\alpha \in [0,1)} F(0, N, 0, \alpha, (x_j)_{j \geq 1}).$$

And, for any real number $\alpha \in (0, 1)$, for any sequence of real numbers $(x_j)_{j \geq 1}$, and for any non-negative integers N and k we have

$$F(0, N, 0, \alpha, (x_j)_{j \geq 1}) \leq N/b^k + \sum_{h=1}^{k}(b - 1) \max_{0 \leq a < b^h} F(0, N, ab^{-h}, (a + 1)b^{-h}, (x_j)_{j \geq 1}).$$

This observation follows from the fact that every interval $[0, \alpha)$ can be covered by at most $(b - 1)$ intervals of length b^{-1}, at most $(b - 1)$ intervals of length b^{-2}, and so on, at most $(b - 1)$ intervals of length b^{-k}, and finally one additional interval of length b^{-k}. This decomposition can be easily derived from the digital representation of α in base b.

The index set can be decomposed in intervals between powers of 2, and every possible initial segment of the index set can be written as a disjoint union of such sets. This fact is expressed in the following lemma.

Lemma 7 (adapted from [10, Lemma 4]). *Let $b \geq 2$ be an integer, let N be a positive integer and let n be such that $2^{n-1} < N \leq 2^n$, and let M be a non-negative integer. Then, there are non-negative integers $m_1, \ldots, m_n$ such that $m_\ell 2^\ell + 2^{\ell-1} \leq N$ for $\ell = 1, \ldots, n$, and such that for any positive integer h and any a, with $0 \leq a < b^h$,*

$$F(M, N, ab^{-h}, (a + 1)b^{-h}, \{b^j x\}_{j \geq 0})$$
$$\leq N^{1/2} + \sum_{n/2 \leq \ell \leq n} F(M + m_\ell 2^\ell, 2^{\ell-1}, ab^{-h}, (a + 1)b^{-h}, \{b^j x\}_{j \geq 0}).$$

For the proof of Theorem 1 we proceed by induction, and define a sequence of nested binary intervals $(\Omega_k)_{k \geq 1}$ which gives us the binary digits of the absolutely normal number which we want to construct. Set $\Omega_1 = \Omega_2 = \cdots = \Omega_{99} = (0, 1)$ for the start of the induction. (We start the induction at $k = 100$ in order to avoid trivial notational problems with small values of k.) We will always assume that $b \leq k$, so in step k only bases b from 2 up to k are considered. Different bases are added gradually as the induction steps forward.

For integers $k \geq 100$ and b such that $2 \leq b \leq k$ we set

$$N_k^{(b)} = \left\lceil 2^k \frac{\log 2}{\log b} \right\rceil.$$

We define sets

$$\mathcal{N}_k^b = \left\{ N \in \mathbb{N} : \ N_k^{(b)} + 4k < N \leq N_{k+1}^{(b)} \right\}, \qquad k \geq 100, \ 2 \leq b \leq k,$$

and

$$\mathcal{R}_k^b = \left\{ N \in \mathbb{N} : \ N_k^{(b)} < N \leq N_k^{(b)} + 4k \right\}, \qquad k \geq 100, \ 2 \leq b \leq k.$$

The indices in $\bigcup_k \mathcal{R}_k^b$ are the "remainder", and do not give a relevant contribution. Their purpose is to separate the elements of $\mathcal{N}_k^b$ from those of $\mathcal{N}_{k+1}^b$, so that b^{j_2} is significantly larger than b^{j_1} whenever $j_2 \in \mathcal{N}_{k+1}^b$ and $j_1 \in \mathcal{N}_k^{(b)}$. The sets $\mathcal{N}_k^b$ and $\mathcal{R}_k^b$ are constructed in such a way that they form a partition of $\mathbb{N}$, except for finitely many initial elements of $\mathbb{N}$. Precisely, one can check that these sets form a partition of $\mathbb{N} \setminus \left\{ 1, \dots, N_{\max\{100,b\}}^b \right\}$.

For the induction step, assume that $k \geq 100$ and that the interval Ω_{k-1} is already defined, and that the length of Ω_{k-1} is bounded below by

$$(2) \qquad\qquad\qquad\qquad \mu(\Omega_{k-1}) \geq 2^{-2^k - k}.$$

Set

$$n_k^{(b)} = \left\lceil \log_2 \left(N_{k+1}^{(b)} - N_k^{(b)} - 4k \right) \right\rceil.$$

and

$$T_b(k) = \left\lceil \frac{n_k^{(b)} \log 2}{2 \log b} \right\rceil.$$

For non-negative integers b, a, h, ℓ such that

$$2 \leq b \leq k, \quad 0 \leq a < b^h, \quad 1 \leq h \leq T_b(k), \quad n_k^{(b)}/2 \leq \ell \leq n_k^{(b)},$$

and non-negative integers m_ℓ such that

$$(3) \qquad\qquad\qquad N_k^{(b)} + 4k + m_\ell 2^\ell + 2^{\ell-1} \leq N_{k+1}^{(b)}$$

we define the sets

$$H(b, k, a, h, \ell, m_\ell) = \left\{ x \in \Omega_{k-1} : F\left(N_k^{(b)} + 4k + m_\ell 2^\ell, 2^{\ell-1}, ab^{-h}, (a+1)b^{-h}, \{b^j x\}_{j \geq 0} \right) \right.$$
$$\left. > 46 \cdot 2^{(\ell-1)/2} h^{-3/2} (n_k^{(b)} - \ell + 1)^{1/2} \right\}.$$

Furthermore, set

$$H_{b,k} = \bigcup_{h=1}^{T_b(k)} \bigcup_{a=0}^{b^h - 1} \bigcup_{n_k^{(b)}/2 \leq \ell \leq n_k^{(b)}} \bigcup_{m_\ell} H(b, k, a, h, \ell, m_\ell).$$

where the last union is over those $m_\ell \geq 0$ satisfying (3).

The following lemma gives an upper bound for the measure of the set $H_{b,k}$. The proof of the lemma will be given in Section 3 below.

Lemma 8. *For $k \geq 100$ and $2 \leq b \leq k$ we have*

$$\frac{\mu(H_{b,k})}{\mu(\Omega_{k-1})} \leq \frac{1}{2^b}.$$

As in the proof of Lemma 3, let $\mathbf{1}_{[ab^{-h},(a+1)b^{-h})}(x)$ denote the indicator function of the interval $[ab^{-h},(a+1)b^{-h})$. For the function F appearing in the definition of $H(b,k,a,h,\ell,m_\ell)$, we can write

(4)
$$F\left(N_k^{(b)} + 4k + m2^\ell, 2^{\ell-1}, ab^{-h}, (a+1)b^{-h}, (\{b^j x\})_{j\geq 0}\right)$$

$$= \left| \sum_{j=N_k^{(b)}+4k+m2^\ell}^{N_k^{(b)}+4k+m2^\ell+2^{\ell-1}-1} \left(\mathbf{1}_{[ab^{-h},(a+1)b^{-h})}(\{b^j x\}) - b^{-h}\right) \right|.$$

Note that the function $\mathbf{1}_{[ab^{-h},(a+1)b^{-h})}(x)$ is a step function which is constant on intervals ranging from one integer multiple of b^{-h} to the next (it is zero everywhere, except from ab^{-h} to $(a+1)b^{-h}$, where it is one). Accordingly, for some j, the function

$$\mathbf{1}_{[ab^{-h},(a+1)b^{-h})}(\{b^j x\})$$

is a step function which is constant on intervals ranging from one integer multiple of $b^{-h}b^{-j}$ to the next. Thus the function in line (4) is constant on all intervals ranging from one integer multiple of $b^{-h}b^{-(N_k^{(b)}+4k+m2^\ell+2^{\ell-1}-1)}$ to the next, and thus by $h \leq T_b(k)$ and by (3) it is also constant on all intervals ranging from one integer multiple of $b^{-T_b(k)}b^{-N_{k+1}^{(b)}}$ to the next.

As a consequence, the set $H_{b,k}$ consists of intervals whose left and right endpoints are integer multiples of

(5)
$$b^{-T_b(k)}b^{-N_{k+1}^{(b)}} = b^{-\left\lceil \frac{n_k^{(b)}\log 2}{2\log b} \right\rceil} b^{-\left\lceil \frac{2^{k+1}\log 2}{\log b} \right\rceil}.$$

We call these intervals "elementary intervals". We have

$$b^{-\left\lceil \frac{n_k^{(b)}\log 2}{2\log b} \right\rceil} \geq 2^{-n_k^{(b)}/2}b^{-1} \geq 2^{-(\log_2 N_{k+1}^{(b)})/2-1}b^{-1} \geq 2^{-k/2-2}b^{-1},$$

and

$$b^{-\left\lceil \frac{2^{k+1}\log 2}{\log b} \right\rceil} \geq 2^{-2^{k+1}}b^{-1},$$

So the length of these elementary intervals of $H_{b,k}$ is at least $2^{-2^{k+1}-k/2-2}b^{-2}$.

Let $H_{b,k}^*$ denote the collection of all those intervals of the form

(6)
$$\left[a2^{-2^{k+1}-k}, (a+1)2^{-2^{k+1}-k}\right) \qquad \text{for some integer } a$$

which have non-empty intersection with $H_{b,k}$. Note that by the calculations in the previous paragraph the intervals of the form (6) are much shorter than the elementary

intervals of $H_{b,k}$, and thus the total measure of $H^*_{b,k}$ is just a little bit larger than that of $H_{b,k}$. In particular, it is true that

$$\mu(H^*_{b,k}) \leq \frac{11}{10}\mu(H_{b,k}).$$

Consequently, by Lemma 8 we have

$$\mu\left(\Omega_{k-1}\backslash\bigcup_{b=2}^{k} H^*_{b,k}\right) \geq \left(1 - \frac{11}{10}\sum_{b=2}^{k}\frac{1}{2^b}\right)\mu(\Omega_{k-1}) \geq \frac{9}{20}\mu(\Omega_{k-1}).$$

Thus, there exists an interval of the form (6) which is contained in Ω_{k-1}, but has empty intersection with all the sets $H_{b,k}$ for $b = 2, \ldots, k$. We define Ω_k as this interval, and note that the length of Ω_k is

(7) $$\mu(\Omega_k) = 2^{-2^{k+1}-k}.$$

Now we can make the induction step $k \mapsto k+1$, where (7) guarantees that the induction hypothesis (2) is met.

3   Proof of Lemma 8

We use Corollary 5 to estimate the measure of the sets $H(b, k, a, h, \ell, m_\ell)$. More precisely, we apply the corollary with the choice of

$$j_0 = N_k^{(b)}+4k, \qquad M = m_\ell 2^\ell, \qquad N = 2^{\ell-1}, \qquad A = \Omega_{k-1}, \qquad \varepsilon = 46(n_k^{(b)}-\ell+1)^{1/2}h^{-2},$$

where

$$1 \leq h \leq T_b(k), \qquad n_k^{(b)}/2 \leq \ell \leq n_k^{(b)},$$

and m_ℓ satisfies (3). So,

$$\varepsilon\sqrt{hN} = 46 \cdot 2^{(\ell-1)/2}h^{-3/2}(n_k^{(b)}-\ell+1)^{1/2}.$$

For the corollary to be applicable, we have to check whether $N \geq h$ and (1) hold for our choice of variables. However, both conditions are easily seen to be satisfied, since by assumption we have $N \geq 2^{n_k^{(b)}/2-1}$, which depends on k exponentially, while $h \leq T_b(k) \leq \left\lceil\frac{n_k^{(b)}\log 2}{2\log b}\right\rceil$ and $\varepsilon \leq 46\sqrt{n_k^{(b)}}$ grow in k at most linearly (remember that we assumed $k \geq 100$). Thus, we can apply Corollary 5, and we obtain

$$\begin{aligned}\mu(H(b, k, a, h, \ell, m_\ell)) &\leq \mu(\Omega_{k-1})2h\exp\left(-\frac{46^2 b(n_k^{(b)}-\ell+1)h^{-4}h^5}{529}\right) + 2b^{-j_0} \\ &= \mu(\Omega_{k-1})2h\exp\left(-4b(n_k^{(b)}-\ell+1)h\right) + 2b^{-j_0}.\end{aligned}$$

Note that by (2),

$$2b^{-j_0} = 2b^{-N_k^{(b)}-4k} \leq 2b^{-\frac{2^k\log 2}{\log b}+1-4k} \leq 2b2^{-2^k}b^{-4k} \leq 2b^{-3k+1}\mu(\Omega_{k-1}).$$

Using the facts that $T_b(h) \leq k/2 + 1$, that $n_k^{(b)} \leq k$ for all b, and that (3) implies that there are at most $2^{n_k^{(b)} - \ell} \leq 2^k$ different values for m_ℓ, we obtain

$$\sum_{h=1}^{T_b(k)} \sum_{a=0}^{b^h-1} \sum_{n_k^{(b)}/2 \leq \ell \leq n_k^{(b)}} \sum_{m_\ell} 2b^{-3k+1}$$

$$\leq (k/2 + 1)b^{k/2+1}k2^k2b^{-3k+1}$$

$$\leq \frac{1}{10}b^{-k},$$

where for the last inequality we use the fact that $k \geq 100$ (by assumption).

Furthermore, using the fact that $e^{-xy} \leq e^{-x}e^{-y}$ for $x, y \geq 2$, we have

$$\sum_{h=1}^{T_b(k)} \sum_{a=0}^{b^h-1} \sum_{n_k^{(b)}/2 \leq \ell \leq n_k^{(b)}} \sum_{m_\ell} 2h \exp\left(-4bh(n_k^{(b)} - \ell + 1)\right)$$

$$\leq \sum_{h=1}^{T_b(k)} b^h \sum_{n_k^{(b)}/2 \leq \ell \leq n_k^{(b)}} 2^{n_k^{(b)} - \ell} 2h \exp(-2bh) \exp\left(-2(n_k^{(b)} - \ell + 1)\right)$$

$$\leq \underbrace{\left(\sum_{h=1}^{\infty} 2hb^h \exp(-2bh)\right)}_{\leq 11/10 e^{-b}} \underbrace{\sum_{n_k^{(b)}/2 \leq \ell \leq n_k^{(b)}} \exp\left(-(n_k^{(b)} - \ell + 1)\right)}_{\leq \sum_{r=1}^{\infty} e^{-r} \leq 6/10}$$

$$\leq \frac{7}{10}e^{-b},$$

where we used that $b - \log b \geq 1.3$ for $b \geq 2$ and consequently

$$\sum_{h=1}^{\infty} 2hb^h e^{-2bh} = \sum_{h=1}^{\infty} 2he^{-h(b-\log b)}e^{-bh} \leq e^{-b} \underbrace{\sum_{h=1}^{\infty} 2he^{-1.3h}}_{\leq 11/10} \leq \frac{11}{10}e^{-b}.$$

Thus, we have

$$\mu(H_{b,k}) \leq \frac{7}{10}e^{-b}\mu(\Omega_{k-1}) + \frac{1}{10}b^{-k}\mu(\Omega_{k-1})$$

$$\leq 2^{-b}\mu(\Omega_{k-1}),$$

where we used the assumption that $b \leq k$. This proves the lemma.

4 Proof of Theorem 1

The proof of Theorem 1 now follows using well-known arguments, which allow to turn the estimates for subsums over dyadic subsets of the index set and over dyadic subintervals of the unit interval into a result which holds uniformly over all subintervals in the unit interval, and for all initial segments of the full index set.

Let $b \geq 2$ be given, and assume that N is "large" (depending on b). Then there is a number k such that N is contained in either $\mathcal{N}_k^b$ or $\mathcal{R}_k^b$. Let x be a real number which

is contained in $\bigcap_{j\geq 1}\Omega_j$. Such a number exists, since $(\Omega_j)_{j\geq 1}$ is a sequence of non-empty nested intervals. Then for this x we have, for arbitrary $0 \leq \alpha_1 < \alpha_2 \leq 1$,

$$F(0, N, \alpha_1, \alpha_2, \{b^j x\}_{j\geq 1}) \quad \leq$$

$$(8) \qquad\qquad F(0, N^{(b)}_{\lfloor k/2\rfloor}, \alpha_1, \alpha_2, (\{b^j x\})_{j\geq 0})$$

$$(9) \qquad\qquad + \sum_{r=\lfloor k/2\rfloor}^{k-1} F(N^{(b)}_r + 4r, N^{(b)}_{r+1} - (N^{(b)}_r + 4r), \alpha_1, \alpha_2, \{b^j x\}_{j\geq 0})$$

$$(10) \qquad\qquad + F(N^{(b)}_k, N - N^{(b)}_k - 4k, \alpha_1, \alpha_2, \{b^j x\}_{j\geq 0})$$

$$(11) \qquad\qquad + \#\left\{ j : j \in \bigcup_k \mathcal{R}^b_k, \ j \leq N \right\}.$$

The term in line (8) is bounded by $N^{(b)}_{\lfloor k/2\rfloor} \leq 2^{k/2\frac{\log 2}{\log b}}+1 \leq 2\sqrt{N}$, since $N > N^{(b)}_k \geq 2^{k\frac{\log 2}{\log b}}$ by assumption. Now we bound the term in line (9). By Remark 6 and Lemma 7 and using the definition of the sets $H_{k,b}$, for every r such that $\lfloor k/2\rfloor \leq r \leq k-1$, we have

$$F(N^{(b)}_r + 4r, N^{(b)}_{r+1} - (N^{(b)}_r + 4r), \alpha_1, \alpha_2, \{b^j x\}_{j\geq 0})$$

$$\leq \sqrt{N^{(b)}_{r+1}} + 2(b-1) \sum_{n^{(b)}_r/2\leq \ell\leq n^{(b)}_r} \sum_{h=1}^{\infty} \max_{0\leq a<b^h} F(N^{(b)}_r + 4r + m_\ell 2^\ell, 2^{\ell-1}, ab^{-h}, (a+1)b^{-h}, \{b^j x\}_{j\geq 0})$$

$$\text{for integers } m_1, m_2, \dots m_{n^{(b)}_r} \text{ established in Lemma 7,}$$

$$\leq \sqrt{N^{(b)}_{r+1}} + 2(b-1) \sum_{n^{(b)}_r/2\leq \ell\leq n^{(b)}_r} \sum_{h=1}^{\infty} h^{-3/2}46 \cdot 2^{(\ell-1)/2}(n^{(b)}_r - \ell + 1)^{1/2}$$

$$\leq \sqrt{N^{(b)}_{r+1}} + 2(b-1)\cdot 46 \underbrace{\left(\sum_{h=1}^{\infty} h^{-3/2}\right)}_{\leq 2.62} \underbrace{\left(\sum_{n^{(b)}_r/2\leq \ell\leq n^{(b)}_r} 2^{(\ell-1)/2}(n^{(b)}_r - \ell + 1)^{1/2}\right)}_{\leq 2^{n^{(b)}_r/2}\sum_{u=1}^{\infty} 2^{-u/2}u^{1/2}\leq 4.15\cdot 2^{n^{(b)}_r/2}\leq 2.94\sqrt{N^{(b)}_{r+1}}}$$

$$\leq \sqrt{N^{(b)}_{r+1}} + 709\cdot b\sqrt{N^{(b)}_{r+1}}$$

$$\leq 710\cdot b\cdot 2^{(r+1-k)/2}\sqrt{N^{(b)}_k}.$$

Consequently, for the term in line (9) we get

$$\sum_{r=\lfloor k/2\rfloor}^{k-1} F(N^{(b)}_r + 4r, N^{(b)}_{r+1} - (N^{(b)}_r + 4r), \alpha_1, \alpha_2, \{b^j x\}_{j\geq 0}) \leq 711\cdot b \sum_{r=\lfloor k/2\rfloor}^{k-1} 2^{(r+1-k)/2}\sqrt{N^{(b)}_k}$$

$$\leq 2425\cdot b\sqrt{N^{(b)}_k}$$

$$\leq 2425\cdot b\sqrt{N}.$$

Similarly, for the term in line (10) we get

$$F(N^{(b)}_k, N - N^{(b)}_k - 4k, \alpha_1, \alpha_2, \{b^j x\}_{j\geq 0}) \leq 711\cdot b \sqrt{N^{(b)}_{k+1}}$$

$$\leq 1005\cdot b\sqrt{N},$$

where we used the fact that $2N \geq N_{k+1}^{(b)}$.

Finally, the term in line (11) is bounded by $4k\lceil k/2 \rceil \leq \sqrt{N}$ for sufficiently large N.

Concluding our estimates for the lines (8)–(11), we finally get

$$F(0, N, \alpha_1, \alpha_2, \{b^j x\}_{j \geq 0}) \leq (2 + 2425 + 1005 + 1)\, b\sqrt{N} = 3433 \cdot b\sqrt{N},$$

for all sufficiently large N. This can be written in the form

$$D_N((\{b^j x\})_{j \geq 0}) \leq 3433 \cdot b\, N^{-1/2}$$

for sufficiently large N, which proves the theorem.

4.1 Computational complexity

The real number determined by our construction is the unique element x in $\bigcap_{k \geq 1} \Omega_k$. The definition of $(\Omega_k)_{k \geq 1}$ is inductive. Assume that Ω_{k-1} is given. The interval Ω_k is the leftmost interval of the form

$$\left[a 2^{-2^{k+1}-k}, (a+1) 2^{-2^{k+1}-k} \right)$$

that lies in

$$\Omega_{k-1} \setminus \bigcup_{b=2}^{k} H_{b,k}.$$

So, Ω_k is one element of the partition of Ω_{k-1} in 2^{2^k+1} subintervals. Let us count first how many mathematical operations suffice to test if one of these subintervals is outside $\bigcup_{b=2}^{k} H_{b,k}$. Recall that

$$\bigcup_{b=2}^{k} H_{b,k} = \bigcup_{b=2}^{k} \bigcup_{h=1}^{T_b(k)} \bigcup_{a=0}^{b^h-1} \bigcup_{n_k^{(b)}/2 \leq \ell \leq n_k^{(b)}} \bigcup_{m_\ell} H(b, k, a, h, \ell, m_\ell).$$

where the last union is over those $m_\ell \geq 0$ satisfying $N_k^{(b)} + 4k + m_\ell 2^\ell + 2^{\ell-1} \leq N_{k+1}^{(b)}$. There are at most $2^{n_k^{(b)} - \ell}$ values of m_ℓ, and for each of them the evaluation of

$$F(N_k^{(b)} + 4k + m 2^\ell, 2^{\ell-1}, ab^{-h}, (a+1)b^{-h}, \{b^j x\}_{j \geq 0}),$$

for any fixed x and fixed k, b, a, h, requires the inspection at $2^{\ell-1}$ indices. Hence, the total number of indices involved in the inspection is $2^{n_k^{(b)} - \ell} \cdot 2^{\ell-1} = 2^{n_k^{(b)}}$. Observe that $b \leq k$, $T_b(k) < k/2$, $n_k^{(b)} \leq k$, and that there are $k/2$ values of ℓ. Thus, ignoring the operations needed to perform base change, the number of mathematical operations to test if one candidate subinterval is outside $\bigcup_{b=2}^{k} H_{b,k}$ is at most

$$k \cdot k/2 \cdot k^{k/2} 2^k.$$

In the worst case we need to test all the subintervals (except the last one), and there are

$$2^{2^k+1}$$

of them. This last factor dominates the total number of mathematical operations that should be performed in the worst case at step k, which consequently is the order at most $\mathcal{O}\left(2^{2^{k+1}}\right)$, say. Since this is doubly exponential in k, the number of mathematical operations performed from step 1 up to step k is also at most of order $\mathcal{O}\left(2^{2^{k+1}}\right)$.

At step k the construction determines $2^k + 1$ new digits in the binary expansion of the defined number x. Thus, at the end of step k the first 2^{k+1} digits will be determined. Then, to compute the N-th digit in the binary expansion of x it suffices to compute up to step $\lceil \log_2 N \rceil$. This entails a number of mathematical operations that is at most $\mathcal{O}\left(2^{2^{\log N}}\right) = \mathcal{O}\left(2^N\right)$. This proves that there is an algorithm that computes the first N digits of the binary expansion of x after performing a number of operations that is exponential in N.

Acknowledgements

References

[1] Christoph Aistleitner and István Berkes. Limit distributions in metric discrepancy theory. *Monatsh. Math.*, 169(3-4):253–265, 2013.

[2] N. Alvarez and V. Becher. M. Levin's construction of absolutely normal numbers with very low discrepancy. *Mathematics of Computation*, 86(308):2927–2946, 2017.

[3] V. Becher, P.A. Heiber, and T. Slaman. A polynomial-time algorithm for computing absolutely normal numbers. *Information and Computation*, 232:1–9, 2013.

[4] Y. Bugeaud. *Distribution Modulo One and Diophantine Approximation.* Number 193 in Cambridge Tracts in Mathematics. Cambridge University Press, Cambridge, UK, 2012.

[5] K. Fukuyama. The law of the iterated logarithm for discrepancies of $\{\theta^n x\}$. *Acta Mathematica Hungarica*, 118(1):155–170, 2008.

[6] S. Gál and L. Gál. The discrepancy of the sequence $\{(2^n x)\}$. *Koninklijke Nederlandse Akademie van Wetenschappen Proceedings. Seres A 67 = Indagationes Mathematicae*, 26:129–143, 1964.

[7] N. Korobov. On completely uniform distributions and jointly normal numbers. *Izv. AN SSSR, ser. matem.*, 20, 1956.

[8] M. Levin. On absolutely normal numbers. *Vestnik Moskovskogo Universiteta. Seriya 1. Matematika. Mekhanika*, 1:31–37, 87, 1979. English translation in Moscow University Mathematics Bulletin, 34 (1979), no. 1, 32-39.

[9] M. Levin. On the discrepancy estimate of normal numbers. *Acta Arithmetica*, 88:99–111, 1999.

[10] W. Philipp. Limit theorems for lacunary series and uniform distribution mod 1. *Acta Arithmetica*, 26(3):241–251, 1975.

[11] A.-M. Scheerer. Computable absolutely normal numbers and discrepancies. *Mathematics of Computation*, 86(308):2911–2926, 2017.

[12] W. Schmidt. Irregularities of distribution. vii. *Acta Arithmetica*, 21:45–50, 1972.

[13] D. Stroock. *Probability theory, an analytic view*. Cambridge University Press, Cambridge, 1993.

[14] A. van der Vaart and J. Wellner. *Weak convergence and empirical processes*. Springer Series in Statistics. Springer-Verlag, New York, 1996.