ACTA ARITHMETICA
* (201*)

On the construction of absolutely normal numbers

by

Christoph Aistleitner (Graz), Verónica Becher (Buenos Aires),
Adrian-Maria Scheerer (Graz)
and Theodore A. Slaman (Berkeley, CA)

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

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

The sequence $(x_j)_{j\geq 0}$ is *uniformly distributed* 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. The number x is *normal* with respect to an integer base $b \geq 2$ 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 $N \geq N_0(b)$,*

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

We can take $C_b = 3433 \cdot b$. Moreover, there is an algorithm that computes the first N digits of the expansion of x in base 2 after performing exponentially (in N) many 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 $b \geq 2$ the discrepancy of the sequence $(\{b^j x\})_{j\geq 0}$ obeys the law of iterated logarithm. Philipp [10] gave explicit constants. Fukuyama [5, Corollary] sharpened the

2010 *Mathematics Subject Classification*: Primary 11K16; Secondary 11Y16, 68-04.
Key words and phrases: normal numbers, uniform distribution, discrepancy.
Received 13 February 2017; revised 11 July 2017.
Published online *.

result by proving 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, one has

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

To prove Theorem 1 we give a construction of a real number x such that, for every integer $b \geq 2$, $D_N((\{b^j x\})_{j\geq 0})$ 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 $(\Omega_k)_{k\geq 1}$ of nested binary intervals 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 $\bigcap_{k\geq 1} \Omega_k$ is a computable number which satisfies the desired discrepancy estimate. The construction uses just discrete mathematics and directly yields the binary expansion of the number computed. Unfortunately, the algorithm that computes the first N digits performs exponentially 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–Smirnov 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 (called 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,

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

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

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

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 such that there are infinitely many Ns with

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

This lower bound is attained by some so-called low-discrepancy sequences (see [4] and the references there), but there 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
$$D_N(\{b^j x\}_{j\geq 0}) = \mathcal{O}(\psi(N)) \quad \text{as } N \to \infty?$$
- 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 above. Is there a real number x such that for *all* integer bases $b \geq 2$,

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

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

$$\begin{aligned} &F(M, N, \alpha_1, \alpha_2, (x_j)_{j\geq 1}) \\ &\qquad = |\#\{j : M \leq j < M + N : \alpha_1 \leq x_j < \alpha_2\} - (\alpha_2 - \alpha_1)N|. \end{aligned}$$

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

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

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 $X_1, \dots, X_n$ 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 $\varepsilon > 0$,*

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

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 $0 \leq a < b^h$,*

$$\begin{aligned} &\mu\big(\{x \in (0,1) : F(M, N, ab^{-h}, (a+1)b^{-h}, \{b^j x\}_{j\geq 0}) > \varepsilon\sqrt{hN}\}\big) \\ &\qquad\qquad \leq 2h\exp\bigg(\frac{-\varepsilon^2}{2b^{-h}(1-b^{-h}) + 2/3\varepsilon\lfloor N/h\rfloor^{-1/2}}\bigg). \end{aligned}$$

Proof. We split the index set $\{M, M+1, \dots, M+N-1\}$ into h classes, according to the remainder modulo h. Then each of these classes contains either $\lfloor N/h\rfloor$ or $\lceil N/h\rceil$ elements. Let $\mathbf{1}_A$ denote the indicator function of the set A. Let $\mathcal{M}_0$ denote the class of all indices in $\{M, \dots, M+N-1\}$ which are zero modulo h. Set $n_0 = \#\mathcal{M}_0$. Then it is an easy exercise to check that the system of functions $(\mathbf{1}_{[ab^{-h},(a+1)b^{-h})}(\{b^j x\}) - b^{-h})_{j\in\mathcal{M}_0}$ 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

$$\mu\Big(\Big\{x \in (0,1) : \Big| \sum_{j\in\mathcal{M}_0} (\mathbf{1}_{[ab^{-h},(a+1)b^{-h})}(\{b^j x\}) - b^{-h})\Big| > \varepsilon\sqrt{n_0}\Big\}\Big) \le 2\exp\bigg(\frac{-\varepsilon^2}{2b^{-h}(1-b^{-h}) + 2/3\varepsilon n_0^{-1/2}}\bigg).$$

Clearly, similar estimates hold for the other residue classes. Let $n_1, \dots, n_{h-1}$ denote the cardinalities of these classes. By assumption $n_0 + \dots + n_{h-1} = N$. By the Cauchy–Schwarz inequality we have $\sqrt{n_0} + \dots + \sqrt{n_{h-1}} \le \sqrt{h}\sqrt{N}$. Thus, summing up, we obtain

$$\mu\Big(\Big\{x \in (0,1) : \Big|\Big(\sum_{j=M}^{M+N-1} \mathbf{1}_{[ab^{-h},(a+1)b^{-h})}(\{b^j x\})\Big) - Nb^{-h}\Big| > \varepsilon\sqrt{hN}\Big\}\Big) \le 2h\exp\bigg(\frac{-\varepsilon^2}{2b^{-h}(1-b^{-h}) + 2/3\varepsilon\lfloor N/h\rfloor^{-1/2}}\bigg). \ \blacksquare$$

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

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

$$\mu\big(\big\{x \in A : F(M+j_0, N, ab^{-h}, (a+1)b^{-h}, \{b^j x\}_{j\ge 0}) > \varepsilon\sqrt{hN}\big\}\big) \le 2\mu(A)h\exp\bigg(\frac{-\varepsilon^2}{2b^{-h}(1-b^{-h}) + 2/3\varepsilon\lfloor N/h\rfloor^{-1/2}}\bigg) + 2b^{-j_0}.$$

Proof. Let B denote the largest interval contained in A with both endpoints being integer multiples of b^{-j_0}. Then $\mu(A \setminus B) \le 2b^{-j_0}$. Furthermore, by periodicity we have

$$\begin{aligned}\mu\big(\big\{x \in B : F(M+j_0, N, ab^{-m}, (a+1)b^{-m}, \{b^j x\}_{j\ge 0}) > \varepsilon\sqrt{hN}\big\}\big) \\ = \mu(B)\cdot\mu\big(\big\{x \in (0,1) : F(M, N, ab^{-m}, (a+1)b^{-m}, \{b^j x\}_{j\ge 0}) > \varepsilon\sqrt{hN}\big\}\big),\end{aligned}$$

for which we can apply Lemma 3. Note that $\mu(B) \le \mu(A)$. ∎

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

$$\frac{2}{3}\varepsilon\lfloor N/h\rfloor^{-1/2} \le \frac{1}{bh^5}. \tag{1}$$

[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.

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*,*

$$\mu\big(\{x \in A : F(M+j_0, N, ab^{-h}, (a+1)b^{-h}, \{b^j x\}_{j\geq 0}) > \varepsilon\sqrt{hN}\}\big) \\ \leq \mu(A) 2h \exp\bigg(\frac{-\varepsilon^2 bh^5}{529}\bigg) + 2b^{-j_0}.$$

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

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

for all $b \geq 2$ and $h \geq 1$ (for the second inequality above 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 $2b^{-h}(1-b^{-h}) + \frac{2}{3}\varepsilon\lfloor N/h\rfloor^{-1/2} \leq 529b^{-1}h^{-5}$. ∎

Remark 6. For any $0 \leq \alpha_1 < \alpha_2 < 1$, 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 $\alpha \in (0,1)$, for any sequence $(x_j)_{j\geq 1}$ of real numbers, 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 $b^{-2}, \ldots,$ 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 into 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, 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 for any positive integer* h *and any* a *with* $0 \leq a < b^h$*,*

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

For the proof of Theorem 1 we proceed by induction, and define a sequence $(\Omega_k)_{k\geq 1}$ of nested binary intervals which gives us the binary digits of the absolutely normal number which we want to construct. Set $\Omega_1 = \cdots = \Omega_{99} = (0,1)$ to start the induction. (We start 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 proceeds.

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

$$
\begin{aligned}
\mathcal{N}_k^b &= \{N \in \mathbb{N} : N_k^{(b)} + 4k < N \leq N_{k+1}^{(b)}\}, \quad k \geq 100,\ 2 \leq b \leq k, \\
\mathcal{R}_k^b &= \{N \in \mathbb{N} : N_k^{(b)} < N \leq N_k^{(b)} + 4k\}, \quad k \geq 100,\ 2 \leq b \leq k.
\end{aligned}
$$

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 $\mathcal{R}_k^b$ form a partition of $\mathbb{N}$ except for finitely many initial elements; precisely, they form a partition of $\mathbb{N} \setminus \{1, \ldots, N^b_{\max\{100,b\}}\}$.

For the induction step, assume that $k \geq 100$ and Ω_{k-1} is already defined with

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

Set

$$
n_k^{(b)} = \lceil \log_2(N_{k+1}^{(b)} - N_k^{(b)} - 4k) \rceil \quad \text{and} \quad T_b(k) = \left\lceil \frac{n_k^{(b)} \log 2}{2 \log b} \right\rceil.
$$

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

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

we define

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

Furthermore, set

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

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

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

Lemma 8. *For $k \ge 100$ and $2 \le b \le k$ we have*

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

For the function F appearing in the definition of $H(b,k,a,h,\ell,m_\ell)$, we can write

$$(4)\qquad F(N_k^{(b)} + 4k + m2^\ell, 2^{\ell-1}, ab^{-h}, (a+1)b^{-h}, (\{b^j x\})_{j\ge 0}) = \Bigg| \sum_{j=N_k^{(b)}+4k+m2^\ell}^{N_k^{(b)}+4k+m2^\ell+2^{\ell-1}-1} (\mathbf{1}_{[ab^{-h},(a+1)b^{-h})}(\{b^j x\}) - b^{-h}) \Bigg|.$$

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

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

is a step function which is constant on intervals ranging from one integer multiple of $b^{-h}b^{-j}$ to the next. Thus F in (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 $h \le T_b(k)$ 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, $H_{b,k}$ consists of intervals whose left and right endpoints are integer multiples of

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

We call these intervals *elementary*. We have

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

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

so the total 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

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

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 larger than that of $H_{b,k}$. In particular,

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

Consequently, by Lemma 8 we have

$$\mu\Big(\Omega_{k-1} \setminus \bigcup_{b=2}^{k} H^*_{b,k}\Big) \ge \Big(1 - \tfrac{11}{10}\sum_{b=2}^{k}\frac{1}{2^b}\Big)\mu(\Omega_{k-1}) \ge \tfrac{9}{20}\mu(\Omega_{k-1}).$$

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 $b = 2,\dots,k$. We define Ω_k to be this interval, and note that

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

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

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

where

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

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

$$\mu(H(b,k,a,h,\ell,m_\ell)) \le \mu(\Omega_{k-1}) 2h \exp\Big(-\frac{46^2 b(n_k^{(b)}-\ell+1)h^{-4}h^5}{529}\Big) + 2b^{-j_0}$$
$$= \mu(\Omega_{k-1}) 2h \exp(-4b(n_k^{(b)}-\ell+1)h) + 2b^{-j_0}.$$

Note that by (2),

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

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

$$\sum_{h=1}^{T_b(k)} \sum_{a=0}^{b^h-1} \sum_{n_k^{(b)}/2 \le \ell \le n_k^{(b)}} \sum_{m_\ell} 2b^{-3k+1} \le (k/2+1) b^{k/2+1} k 2^k 2b^{-3k+1} \le \tfrac{1}{10} b^{-k},$$

where for the last inequality we again use the assumption $k \ge 100$.

Furthermore, from the fact that $e^{-xy} \le e^{-x}e^{-y}$ for $x, y \ge 2$, we have

$$\sum_{h=1}^{T_b(k)} \sum_{a=0}^{b^h-1} \sum_{n_k^{(b)}/2 \le \ell \le n_k^{(b)}} \sum_{m_\ell} 2h \exp(-4bh(n_k^{(b)}-\ell+1))$$
$$\le \sum_{h=1}^{T_b(k)} b^h \sum_{n_k^{(b)}/2 \le \ell \le n_k^{(b)}} 2^{n_k^{(b)}-\ell}\, 2h \exp(-2bh) \exp(-2(n_k^{(b)}-\ell+1))$$
$$\le \underbrace{\Big(\sum_{h=1}^{\infty} 2hb^h \exp(-2bh)\Big)}_{\le 11e^{-b}/10} \underbrace{\sum_{n_k^{(b)}/2 \le \ell \le n_k^{(b)}} \exp(-(n_k^{(b)}-\ell+1))}_{\le \sum_{r=1}^{\infty} e^{-r} \le 6/10} \le \tfrac{7}{10} e^{-b},$$

where we have used $b - \log b \ge 1.3$ for $b \ge 2$. Consequently,

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

Thus,

$$\mu(H_{b,k}) \le \tfrac{7}{10} e^{-b} \mu(\Omega_{k-1}) + \tfrac{1}{10} b^{-k} \mu(\Omega_{k-1}) \le 2^{-b} \mu(\Omega_{k-1})$$

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

4. Proof of Theorem 1. The proof of Theorem 1 now follows using well-known arguments, which allow us 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.

Fix $b \geq 2$, 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 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 arbitrary $0 \leq \alpha_1 < \alpha_2 \leq 1$,

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

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

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

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

$$+ \#\Big\{ j : \; j \in \bigcup_k \mathcal{R}_k^b, \; j \leq N \Big\}. \tag{11}$$

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

$$\begin{aligned}
&F(N_r^{(b)} + 4r, N_{r+1}^{(b)} - (N_r^{(b)} + 4r), \alpha_1, \alpha_2, \{b^j x\}_{j \geq 0}) \\
&\leq \sqrt{N_{r+1}^{(b)}} + 2(b-1) \sum_{n_r^{(b)}/2 \leq \ell \leq n_r^{(b)}} \sum_{h=1}^{\infty} \max_{0 \leq a < b^h} F\big(N_r^{(b)} + 4r + m_\ell 2^\ell, 2^{\ell-1}, ab^{-h}, \\
&\qquad\qquad (a+1)b^{-h}, \{b^j x\}_{j \geq 0}\big) \\
&\qquad\qquad \text{(for } m_1, \ldots, m_{n_r^{(b)}} \text{ as in Lemma 7)} \\
&\leq \sqrt{N_{r+1}^{(b)}} + 2(b-1) \sum_{n_r^{(b)}/2 \leq \ell \leq n_r^{(b)}} \sum_{h=1}^{\infty} h^{-3/2} 46 \cdot 2^{(\ell-1)/2} (n_r^{(b)} - \ell + 1)^{1/2} \\
&\leq \sqrt{N_{r+1}^{(b)}} + 2(b-1) \cdot 46 \underbrace{\Big(\sum_{h=1}^{\infty} h^{-3/2} \Big)}_{\leq 2.62} \\
&\qquad \times \underbrace{\Big(\sum_{n_r^{(b)}/2 \leq \ell \leq n_r^{(b)}} 2^{(\ell-1)/2} (n_r^{(b)} - \ell + 1)^{1/2} \Big)}_{\leq 2^{n_r^{(b)}/2} \sum_{u=1}^{\infty} 2^{-u/2} u^{1/2} \leq 4.15 \cdot 2^{n_r^{(b)}/2} \leq 2.94 \sqrt{N_{r+1}^{(b)}}} \\
&\leq \sqrt{N_{r+1}^{(b)}} + 709 \cdot b \sqrt{N_{r+1}^{(b)}} \leq 710 \cdot b \cdot 2^{(r+1-k)/2} \sqrt{N_k^{(b)}}.
\end{aligned}$$

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

$$\sum_{r=\lfloor k/2 \rfloor}^{k-1} F(N_r^{(b)} + 4r, N_{r+1}^{(b)} - (N_r^{(b)} + 4r), \alpha_1, \alpha_2, \{b^j x\}_{j \geq 0})$$
$$\leq 711 \cdot b \sum_{r=\lfloor k/2 \rfloor}^{k-1} 2^{(r+1-k)/2} \sqrt{N_k^{(b)}} \leq 2425 \cdot b \sqrt{N_k^{(b)}} \leq 2425 \cdot b \sqrt{N}.$$

Similarly, for the term in line (10) we find that

$$F(N_k^{(b)}, N - N_k^{(b)} - 4k, \alpha_1, \alpha_2, \{b^j x\}_{j \geq 0}) \leq 711 \cdot b \sqrt{N_{k+1}^{(b)}} \leq 1005 \cdot b \sqrt{N},$$

where we have 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 (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

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

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} into 2^{2^k+1} subintervals. Let us first count 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

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

for any fixed x and fixed k, b, a, h, requires the inspection of $2^{\ell-1}$ 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 there are $k/2$ values of ℓ. Thus, ignoring the operations needed to perform base change, the number of operations to test whether 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 dominates the total number of mathematical operations that should be performed in the worst case at step k, which consequently is of order at most $\mathcal{O}(2^{2^{k+1}})$, 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 $\mathcal{O}(2^{2^{k+1}})$.

At step k the construction determines $2^k + 1$ new digits in the binary expansion of x. Thus, at the end of step k the first 2^{k+1} digits will be determined. Then, to compute the Nth digit in the binary expansion it suffices to compute up to step $\lceil \log_2 N \rceil$. This entails at most $\mathcal{O}(2^{2^{\log N}}) = \mathcal{O}(2^N)$ operations. In conclusion, there is an algorithm that computes the first N digits of the binary expansion of x and whose number of operations is exponential in N.

Acknowledgements. We thank Yann Bugeaud and Katusi Fukuyama for comments concerning this paper. The first author is supported by the Austrian Science Fund FWF, project Y-901. The second author is supported by ANPCyT project PICT 2014-3260. The third author is supported by FWF projects I 1751-N26, W1230, Doctoral Program "Discrete Mathematics" and SFB F 5510-N26. The fourth author is partially supported by the National Science Foundation grant DMS-1600441. This work was initiated during a workshop on normal numbers at the Erwin Schrödinger Institute in Vienna, Austria, which was held in November 2016 and in which all four authors participated.

References

[1] C. Aistleitner and I. Berkes, *Limit distributions in metric discrepancy theory*, Monatsh. Math. 169 (2013), 253–265.

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

[3] V. Becher, P. Heiber, and T. Slaman, *A polynomial-time algorithm for computing absolutely normal numbers*, Inform. and Comput. 232 (2013), 1–9.
[4] Y. Bugeaud, *Distribution Modulo One and Diophantine Approximation*, Cambridge Tracts in Math. 193, Cambridge Univ. Press, Cambridge, 2012.
[5] K. Fukuyama, *The law of the iterated logarithm for discrepancies of* $\{\theta^n x\}$, Acta Math. Hungar. 118 (2008), 155–170.
[6] S. Gál and L. Gál, *The discrepancy of the sequence* $\{(2^n x)\}$, Nederl. Akad. Wetensch. Proc. Ser. A 67 = Indag. Math. 26 (1964), 129–143.
[7] N. Korobov, *On completely uniform distribution and jointly normal numbers*, Izv. Akad. Nauk SSSR Ser. Mat. 20 (1956), 649–660 (in Russian).
[8] M. Levin, *On absolutely normal numbers*, Vestnik Moskov. Univ. Ser. Mat. Mekh. 1979, no. 1, 31–37 (in Russian); English transl.: Moscow Univ. Math. Bull. 34 (1979), no. 1, 32–39.
[9] M. Levin, *On the discrepancy estimate of normal numbers*, Acta Arith. 88 (1999), 99–111.
[10] W. Philipp, *Limit theorems for lacunary series and uniform distribution mod 1*, Acta Arith. 26 (1975), 241–251.
[11] A.-M. Scheerer, *Computable absolutely normal numbers and discrepancies*, Math. Comput. 86 (2017), 2911–2926.
[12] W. Schmidt, *Irregularities of distribution. VII*, Acta Arith. 21 (1972), 45–50.
[13] D. Stroock, *Probability Theory. An Analytic View*, Cambridge Univ. Press, Cambridge, 1993.
[14] A. van der Vaart and J. Wellner, *Weak Convergence and Empirical Processes*, Springer Ser. Statist., Springer, New York, 1996.

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

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

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

Abstract (will appear on the journal's web site only)

We give a construction of an absolutely normal real number x such that for every integer $b \geq 2$, 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 has not been known before.