Universidad de Buenos Aires
Facultad de Ciencias Exactas y Naturales
Departamento de Computación

Very fast normal numbers

Tesis de Licenciatura en Ciencias de la Computación

Pablo Andrés Gauna
gaunapablo@gmail.com

Directora: Verónica Becher

Buenos Aires, 26 de Noviembre del 2019

Very fast normal numbers

Normality is the most basic form of randomness for real numbers. A real number x is normal to base 2 if in the binary expansion of x the digit 0 occurs with the same limiting frequency as the digit 1, and all blocks of digits of the same length occur with the same limiting frequency. Although almost all real numbers are normal to base 2, some converge to normality faster then others. There is a longstanding open problem about what is the fastest possible speed of convergence to normality for a real number x. This is equivales to ask for the minimal discrepancy that can be achieved by the parametric sequence of the form $(2^n x \mod 1)_{n>0}$, for a real number x. The best results for this problem are due to Mordechay Levin in 1999 who defined constructively two real numbers, x and y, satisfying that the discrepancy of the first N terms of the sequence $(2^n x \mod 1)_{n>0}$ and $(2^n y \mod 1)_{n>0}$ are, respectively, in the order of $(\log N)^2/N$ and $(\log N)^3/N$. In this work we consider Levin's construction for the real number y, and we prove that at each step of the construction there are at least four choices. The proofs is based on paths in the Stern-Brocot tree. We conjecture that the construction yields a number y such that discrepancy of the first N terms of the sequence $(2^n y \mod 1)_{n>0}$ is in the order of $(\log N)^2/N$.

Keywords: Normality, Normal Numbers, Discrepancy, Stern-Brocot tree.

Números normales muy rápidos

Normalidad es la forma más básica de aleatoriedad para números reales. Un número real x es normal en base 2 si en la expansión binaria de x el dígito 0 ocurre, en el límite, con la misma frecuencia que el dígito 1, y todos los bloques de dígitos del mismo tamaño ocurren con la misma frecuencia. A pesar de que casi todos los números reales son normales en base 2, algunos convergen a la normalidad más rápido que otros. Sigue abierta la pregunta de cuál es la velocidad de convergencia a la normalidad más rápida posible para un número real x. Esta pregunta equivale a determinar cuál es la minima discrepancia que puede ser alcanzada por la secuencia paramétrica de la forma $(2^n x \mod 1)_{n>0}$, para un número real x. Los mejores resultados hasta ahora para este probelma fueron dados por Mordechay Levin en 1999 quien define constructivamente dos números reales x e y, tales que la discrepancia de los primeros N términos de la secuencia $(2^n x \mod 1)_{n>0}$ es del orden de $(\log N)^2/N$, y la discrepancia de los primeros N términos de la secuencia $(2^n y \mod 1)_{n>0}$ es del orden $(\log N)^3/N$. En este trabajo nos centramos en la construcción de Levin para el número real y, y probamos que en cada paso de la construcción hay al menos 4 opciones. La prueba esta basada en caminos del árbol Stern-Brocot. Conjeturamos que la construcción para y es tal que la discrepancia de los primeros N términos de la secuencia $(2^n y \mod 1)_{n>0}$ se encuentra en el orden de $(\log N)^2/N$.

Palabras claves: Normalidad, Números normales, discrepancia, árbol Stern-Brocot.

Contents

This thesis was directed jointly by Verónica Becher and Olivier Carton in the context of the Laboratoire International Associé SINFIN, Université Paris -CNRS/Universidad de Buenos Aires-CONICET.

1 Introduction

A real number x is normal to an integer base b if every block of digits in $\{0,\dots,q-1\}$ of the same length occurs in the base q expansion of x with the same limit frequency. The definition of normality is due to Borel [2], a thorough presentation can be read from [4, 10], see also [1]. A longstanding open question on normal numbers is what is the maximum achievable speed of convergence to normality [9].

The property of normality of real numbers as well its speed of convergence are formalized in the theory of uniform distribution modulo 1, see [10, 5, 4]. For a sequence $(x_n)_{n\geq 0}$ of real numbers in the unit interval the discrepancy of the first N elements is

$$D_N((x_n)_{n\geq 0}) = \sup_{\gamma\in[0,1)} \left| \frac{1}{N}\#\Big\{n : 0 \leq n < N \text{ and } x_n < \gamma\Big\} - \gamma \right|.$$

A sequence $(x_n)_{n\geq 0}$ of real numbers in the unit interval is uniformly distributed exactly when $\lim_{N\to\infty} D_N((x_n)_{n\geq 0}) = 0$. In [16] Schmidt shows that there is a constant C such that for every sequence $(x_n)_{n\geq 0}$ of real numbers in the unit interval there are infinitely many Ns such that

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

This lower bound is actually achieved by van der Corput sequences.

We use the Big O notation to describe the limiting behavior of a function when the argument tends towards a particular value or infinity. For f and g real valued functions defined on the positve real numbers and g strictly positive, we write $f(x)$ is $O(g(x))$ if, for all sufficiently large values of x, the absolute value of $f(x)$ is at most a positive constant multiplied by $g(x)$.

We write $\{x\}$ to denote $x - \lfloor x \rfloor$, the fractional part of x. For an integer q greater than 1, a real number x is normal to base q if and only if the sequence $(\{q^n x\})_{n\geq 0}$ is uniformly distributed in the unit interval. For almost all real numbers x, $D_N((\{q^n x\})_{n\geq 0})$ is $O(\sqrt{(\log\log N)/N})$, see [7, 13, 6]. It is still unknown whether the minimal discrepancy $O(\log N)/N)$ can be achieved by some sequence of the form $(\{q^n x\})_{n\geq 0}$ for some real number x [9, 5, 4]. The smallest discrepancy known for sequences of this form is $O((\log N)^2/N)$. This is proved by Levin [11, Theorem 2], by constructing an instance using Sobol-Faure sequences with the Pascal triangle matrix modulo 2. In [1] Levin's construction is characterize with variants of de Bruijn sequences (that they call nested perfect necklaces) and Levin's work is generalized, obtaining a family of numbers x that yield the same discrepancy bound. No other constructions are known to give this small discrepancy.

In Theorem 1 of the same paper [11], Levin constructs the base-q expansion of a number x such that $D_N(\{q^n x\})_{n\geq 1})$ is in $O\big((\log N)^3/N\big)$. We devote the present thesis to this result. We prove that at each step of the construction there are at least four choices that lead to the minimum discrepancy. Moreover, we conjecture that for any of these four choices the defined real number x satsfies that $D_N(\{q^n x\})_{n\geq 1}$ is in $O\big((\log N)^2/N\big)$.

2 Levin's construction

For a real number x let $[a_0(x); a_1(x), a_2(x) \dots]$ be the continued fraction expansion of x with partial quotients $a_i(x)$, where $a_0(x)$ is an integer and for $i > 0$, each $a_i(x)$ is a positive integer. If $x = [a_0(x); a_1(x), \dots, a_n(x)]$ we define $S(x)$ as the sum of all the coefficients except that of the integer part,

$$S(x) = \sum_{i=1}^{n} a_i(x).$$

Using a result of Popov in [14] Levin [11, Lemma 3] proves that there exists a sequence $(b_m)_{m\geq 1}$ of integers and a positive constant K such that for every $m = 1, 2, \dots$

$$\sum_{r=1}^{m} S(b_m/q^r) \leq Km^3.$$

For such a sequence $(b_m)_{m\geq 1}$ Levin [11, Theorem 2] defines the real number α as follows and proves that α is normal to base q with $D_N((\{\alpha q^n\})_{n\geq 0}) = O\left((\log N)^3/N\right)$.

$$\alpha = \sum_{m\geq 1} \frac{1}{q^{n_m}} \sum_{k=0}^{q^m-1} \left\{\frac{b_m k}{q^m}\right\} \frac{1}{q^{mk}}$$

$$\textit{where } n_1 = 0 \textit{ and } n_k = \sum_{r=1}^{k-1} rq^r, \textit{ for } k = 2, 3, \dots$$

To give a graphic view of the construction we depict the expansion of α in base q as the concatenation of $MegaBlock_1$, $MegaBlock_2$, $MegaBlock_3$, ..., where for each m, the $MegaBlock_m$ is $\sum_{k=0}^{q^m-1} \left\{\frac{b_m k}{q^m}\right\} \frac{1}{q^{mk}}$. For each m, the $MegaBlock_m$ consists of the concatenation of $Block_m^k$, for $k = 0, \dots, q^m - 1$. Since the length of $Block_m^k$, is m, the length of $MegaBlock_m$ is mq^m.

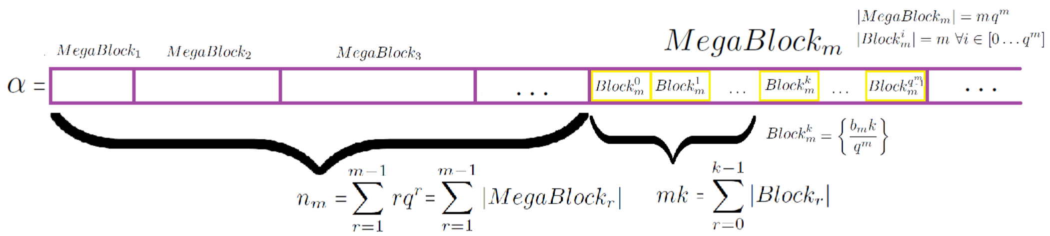

Figure 1: The base q expansion of α pictured as teh contatenation of MegaBlocks.

In the next section we look at the values of the sequence $(b_m)_{m\geq 0}$.

3 There are least four choices for each minimizer

Definition 1 (Minimizer)**.** *Let q be an integer greater than 1. Given a positive integer m, we say that the positive integer b is a minimizer for (m, q) if it minimizes the sum $\sum_{r=1}^{m} S(b/q^r)$.*

Table 1 gives some examples of minimizers and it results. More examples are listed in the Appendix.

	q=2		q=3		q=10	
m	b_m	$sum(b_m)$	b_m	$sum(b_m)$	b_m	$sum(b_m)$
1	1	2	1	3	3	6
2	1	6	2	9	27	17
3	3	11	5	18	173	36
4	3	19	31	29	2627	62
5	5	29	92	44	22627	91
6	19	39	140	63	262113	128
7	37	52	857	85	2262113	170
8	45	67	2570	109	16172177	227
9	151	83	9131	138	226542279	286
10	151	102	12262	172	-	-
11	807	125	31907	207	-	-
12	867	151	46787	245	-	-
13	3367	174	311411	286	-	-
14	3433	201	1288610	332	-	-
15	4825	231	3761986	379	-	-
16	13893	260	-	-	-	-
17	51351	289	-	-	-	-
18	79655	322	-	-	-	-
19	79655	357	-	-	-	-
20	444567	390	-	-	-	-
21	444567	431	-	-	-	-

Table 1: Minimizer b_m for (m, q) and $sum(q, m) = \sum_{r=1}^{m} S(b_m/q^r)$.

We are ready to state the main result of this work.

Theorem 1. *Let q and b be two positive integers coprime such that $q \geq 2$ and let m be an integer such that $b < q^m$. Then, the numbers*

$$\begin{aligned} &b^{(2)} = q^m - b \\ &b^{(3)} \textit{ such that } b^{(3)}b \equiv 1 \pmod{q^m} \textit{ and } 0 < b^{(3)} < q^m \\ &b^{(4)} = q^m - b^{(3)} \end{aligned}$$

satisfy

$$\sum_{r=1}^{m} S(b/q^r) = \sum_{r=1}^{m} S(b^{(i)}/q^r) \textit{ for } i = 2, 3, 4.$$

Thus, if b is a minimizer for (q, m) then $b^{(2)}$, $b^{(3)}$, $b^{(4)}$ are also minimizers for (q, m).

Except for $m = 1, q = 2$, we have $b \neq b^{(2)}$. And experimentally we found that there are a few cases where b is equal to $b^{(3)}$ or $b^{(4)}$ because there are a few b satisfying $b^2 \equiv \pm 1 \pmod{q^m}$ and, for m greater than 3, these cases do not minimze $\sum_{r=1}^{m} S(b/q^r)$.

The rest of this section is devoted to the proof of Theorem 1. The proof of Theorem 1 proves these relationships on the Stern-Brocot tree.

The relationship between the continued fraction $[a_1, .., a_n]$ and its reversed $[a_n, ..., a_1]$ was already known. For instance it appears in B. Adamczewski , J.-P. Allouche [3, Lemma 1], where it is called the mirror formula. It is also reported in Popov [14, Lemma 2].

The relationship between the continued of x and $1 - x$ was also known. It follows from the results by Raney [15]. Since $det(L) = det(R) = 1$ and $det(AB) = det(A)det(B)$ for any matrices A and B, the result follows.

3.1 About the Stern Brocot tree

The proof of Theorem 1 uses the Stern–Brocot tree, which is a binary tree whose vertices correspond one-to-one to the positive rational numbers, see [8]. The root of the Stern–Brocot tree corresponds to the number 1.

The path from the root 1 to a number x in the Stern–Brocot tree (augmented by the values 0/1 and 1/0 that represent infinity) can be found by a binary search using mediants. We can regard the Stern-Brocot tree as a number system for representing rational numbers, because each positive, reduced fraction occurs exactly once. Let's use the letters L and R to stand for going down to the left or right branch as we proceed from the root of the tree to a particular fraction; then, each string of L's and R's uniquely identifies a place in the tree. And converesely, every positive fraction gets represented in this way as a unique string of L's and R's [8]. Figure 2 give the translation functions from sequences of L's and R's and fractions, and conversely.

```
def fraction_to_sbt_path(target_fraction):
    sbt_path = ""
    low, middle, high = Fraction(0, 1), Fraction(1, 1), Fraction(1, 0)
    while middle != target_fraction:
        if target_fraction < middle:
            sbt_path += "L"
            high = middle
        else:
            sbt_path += "R"
            low = middle
        middle = Fraction(
                low.numerator + high.numerator,
                low.denominator + high.denominator)
    return sbt_path
```

```
def sbt_path_to_fraction(path_tree):
    low, middle, high = Fraction(0, 1), Fraction(1, 1), Fraction(1, 0)
    for step in path_tree:
        if step == "L":
            high = middle
        else:
            low = middle
        middle = Fraction(
                low.numerator + high.numerator,
                low.denominator + high.denominator)
    return middle
```

Figure 2: Fraction to SB-tree path and SB-tree path to fraction.

The rows of the Stern Brocot tree have reciprocal symmetry about their center; that is, the j-th term counted from the left is the reciprocal of the j-th term counted from the right. Motivated by this we consider only the left half of the rows. In the sequel we refer to the left half Stern-Brocot tree, and write Half-Stern-Brocot. For a node x in the Half-Stern-Brocot tree we write $SBT\_path(x)$ to the path that goes from the root to x.

Using the matrix notation we can write each node of the Stern-Brocot tree as a 2×2 matrix,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ identifies the node } \frac{a+b}{c+d}.$$

This matrix is obtained by multiplication of matrices depending on the path in the tree, when it goes to the left we multiply by the matrix for L, otherwise by the matrix for R,

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = L \qquad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = R.$$

The initial matrix of the Stern-Brocot tree is the matrix representing its root, which is the identity matrix. The initial matrix for the Half-Stern-Brocot tree is the matrix for L, because it represents its root, which is the fraction $1/2$.

Every positive rational number x can be expressed as a continued fraction of the form $[a_0(x); a_1(x), \ldots, a_k(x)]$ where k and a_0 are non-negative integers, and each subsequent coefficient $a_i(x)$ is a positive integer. The numbers at depth d in the Half-Stern-Brocot tree are the numbers for which the sum of the continued fraction coefficients is $d+2$ see [8]. Thus, for any positive rational number x less than 1,

$$S(x) = length(SBT\_path(x)) + 2$$

3.2 Some lemmas on the paths of the Half-Stern-Brocot

Lemma 2. *For M a matrix that represents a node in the Half-Stern-Brocot tree,*

$$\textit{if } M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \textit{ then } ad - bc = 1.$$

Proof. We prove it by induction on the length of the path.

Inductive Hypothesis. For M a matrix that represents a node in the Half-Stern-Brocot tree,

$$\text{if } M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ then } ad - bc = 1. \tag{1}$$

Base Case. In the Half-Stern-Brocot tree. length is zero with the inicial matrix that represents $1/2$,

$$M = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ then } 1 \times 1 - 0 \times 1 = 1.$$

Inductive step. Path of length n, we add one more step.

Add an R to the path

$$MR = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$$
$$a(c+d) - c(a+b) = ac + ad - ac - cb = ad - cb =_{(1)} 1.$$

Add an L to the path

$$ML = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} a+b & b \\ c+d & d \end{pmatrix}$$
$$(a+b)d - b(c+d) = ad + bd - bc - bd = ad - cb =_{(1)} 1.$$

□

Lemma 3. *Let M be the matrix that represents the node Y/X in the Half-Stern-Brocot tree then*

$$M = \begin{pmatrix} \frac{Y(X-d)+1}{X} & \frac{Yd-1}{X} \\ X-d & d \end{pmatrix}$$

for d a positive integer such that $0 < d < X$ and

$$dY \equiv 1 \pmod{X}.$$

Proof. Let X, Y be given. Assume

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

From Lemma 2 we know $ad - bc = 1$.

$$\begin{aligned}
&\text{Since } X = c + d \text{ then } c = X - d. \\
&\text{Since } Y = a + b \text{ then } a = Y - b. \\
&\text{Since } 1 = ad - bc = ad - b(X-d) = (a+b)d - bX = Yd - bX \\
&\text{ then } b = \frac{Yd-1}{X}. \\
&\text{Since } a = Y - b = Y - \frac{Yd-1}{X} \text{ then } a = \frac{Y(X-d)+1}{X}.
\end{aligned}$$

∎

Lemma 4. *Let $a^{(1)}$ and $b^{(1)}$ be coprime positive integers such that $b^{(1)} < a^{(1)}$. Let $b^{(2)}$, $b^{(3)}$, $b^{(4)}$, $a^{(2)}$, $a^{(3)}$ and $a^{(4)}$ be the integers such that*

$$\begin{aligned}
SBT_path(b^{(2)}/a^{(2)}) &= \text{exchange } L \text{ and } R \text{ in } SBT_path(b^{(1)}/a^{(1)}) \\
SBT_path(b^{(3)}/a^{(3)}) &= \text{reverse } SBT_path(b^{(1)}/a^{(1)}) \\
SBT_path(b^{(4)}/a^{(4)}) &= \text{reverse } SBT_path(b^{(2)}/a^{(2)}).
\end{aligned}$$

Let $M^{(1)}$, $M^{(2)}$, $M^{(3)}$ and $M^{(4)}$ be the matrices that represent the nodes $b^{(1)}/a^{(1)}$, $b^{(2)}/a^{(2)}$, $b^{(3)}/a^{(3)}$, $b^{(4)}/a^{(4)}$ respectively.

$$\begin{aligned}
\text{If} \quad M^{(1)} = LM'^{(1)} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(1,1)} & x^{(1,2)} \\ x^{(2,1)} & x^{(2,2)} \end{pmatrix} \\
\text{then} \quad M^{(2)} = LM'^{(2)} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(2,2)} & x^{(2,1)} \\ x^{(1,2)} & x^{(1,1)} \end{pmatrix} \\
M^{(3)} = LM'^{(3)} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(2,2)} & x^{(1,2)} \\ x^{(2,1)} & x^{(1,1)} \end{pmatrix} \\
M^{(4)} = LM'^{(4)} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(1,1)} & x^{(2,1)} \\ x^{(1,2)} & x^{(2,2)} \end{pmatrix}.
\end{aligned}$$

So,

$$\begin{aligned}
a^{(1)} &= a^{(2)} = a^{(3)} = a^{(4)} = x^{(1,1)} + x^{(1,2)} + x^{(2,1)} + x^{(2,2)} \\
b^{(1)} &= x^{(1,1)} + x^{(1,2)} = a^{(1)} - b^{(2)} \\
b^{(2)} &= x^{(2,2)} + x^{(2,1)} = a^{(1)} - b^{(1)} \\
b^{(3)} &= x^{(2,2)} + x^{(1,2)} = a^{(1)} - b^{(4)} \\
b^{(4)} &= x^{(1,1)} + x^{(2,1)} = a^{(1)} - b^{(3)}.
\end{aligned}$$

Proof. Assume $a^{(1)}, a^{(2)}, a^{(3)}, a^{(4)}$ and $b^{(1)}$, $b^{(2)}$, $b^{(3)}$ and $b^{(4)}$ as in the statement of the lemma. Let $M^{(1)}$, $M^{(2)}$, $M^{(3)}$ and $M^{(4)}$ be the matrices that represent the nodes $b^{(1)}/a^{(1)}$, $b^{(2)}/a^{(2)}$, $b^{(3)}/a^{(3)}$, $b^{(4)}/a^{(4)}$ respectively. We give the proof by induction on the length of the paths.

Inductive Hypothesis:

$$\begin{aligned}
\text{If} \quad M^{(1)} = LM'^{(1)} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(1,1)} & x^{(1,2)} \\ x^{(2,1)} & x^{(2,2)} \end{pmatrix} \\
\text{then} \quad M^{(2)} = LM'^{(2)} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(2,2)} & x^{(2,1)} \\ x^{(1,2)} & x^{(1,1)} \end{pmatrix} \\
M^{(3)} = LM'^{(3)} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(2,2)} & x^{(1,2)} \\ x^{(2,1)} & x^{(1,1)} \end{pmatrix} \\
M^{(4)} = LM'^{(4)} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(1,1)} & x^{(2,1)} \\ x^{(1,2)} & x^{(2,2)} \end{pmatrix}.
\end{aligned}$$

Base case. The path of length 1, L or R that represent $1/3$ and $2/3$ respectively:

$$\begin{aligned}
M^{(1)} = LM'^{(1)} = M^{(3)} = LM'^{(3)} = LL &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \\
M^{(2)} = LM'^{(2)} = M^{(4)} = LM'^{(4)} = LR &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}
\end{aligned}$$

Similarly, the statement also holds for the other base case $M^{(1)} = M^{(3)} = LR$ and $M^{(2)} = M^{(4)} = LL$

Inductive step. Path of length n, we add one more step.
Add an R to the path,

$$\begin{aligned}
LM'^{(1)}R = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(1,1)} & x^{(1,2)} \\ x^{(2,1)} & x^{(2,2)} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(1,1)} & x^{(1,1)} + x^{(1,2)} \\ x^{(2,1)} & x^{(2,1)} + x^{(2,2)} \end{pmatrix} \\
LM'^{(2)}L = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(2,2)} & x^{(2,1)} \\ x^{(1,2)} & x^{(1,1)} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(2,1)} + x^{(2,2)} & x^{(2,1)} \\ x^{(1,1)} + x^{(1,2)} & x^{(1,1)} \end{pmatrix} \\
LRM'^{(3)} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x^{(2,2)} & x^{(1,2)} \\ x^{(2,1)} & x^{(1,1)} \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(2,1)} + x^{(2,2)} & x^{(1,1)} + x^{(1,2)} \\ x^{(2,1)} & x^{(1,1)} \end{pmatrix} \\
LLM'^{(4)} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(1,1)} & x^{(2,1)} \\ x^{(1,2)} & x^{(2,2)} \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(1,1)} & x^{(2,1)} \\ x^{(1,1)} + x^{(1,2)} & x^{(2,1)} + x^{(2,2)} \end{pmatrix}.
\end{aligned}$$

Add an L to the path,

$$\begin{aligned}
LM'^{(1)}L = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(1,1)} & x^{(1,2)} \\ x^{(2,1)} & x^{(2,2)} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(1,1)} + x^{(1,2)} & x^{(1,2)} \\ x^{(2,1)} + x^{(2,2)} & x^{(2,2)} \end{pmatrix} \\
LM'^{(2)}R = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(2,2)} & x^{(2,1)} \\ x^{(1,2)} & x^{(1,1)} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(2,1)} & x^{(2,1)} + x^{(2,2)} \\ x^{(1,1)} & x^{(1,1)} + x^{(1,2)} \end{pmatrix} \\
LLM'^{(3)} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(2,2)} & x^{(1,2)} \\ x^{(2,1)} & x^{(1,1)} \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(2,1)} & x^{(1,1)} \\ x^{(2,1)} + x^{(2,2)} & x^{(1,1)} + x^{(1,2)} \end{pmatrix} \\
LRM'^{(4)} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x^{(1,1)} & x^{(2,1)} \\ x^{(1,2)} & x^{(2,2)} \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x^{(1,1)} + x^{(1,2)} & x^{(2,1)} + x^{(2,2)} \\ x^{(1,2)} & x^{(2,2)} \end{pmatrix}.
\end{aligned}$$

□

Lemma 5. *Let q, b and m be positive integers such that $q \geq 2$ and q and b coprime . Then, for all $r \in \{1, \ldots, m\}$ the lengths of $SBT\_path(\{b/q^r\})$ and $SBT\_path(\{(q^m - b)/q^r\})$ coincide.*

Proof. Observe that for each $r \in \{1, \ldots, m\}$, taking $n = m - r$:

$$\left\{\frac{q^m - b}{q^r}\right\} = \left\{\frac{q^{r+n} - b}{q^r}\right\} = \left\{q^n - \frac{b}{q^r}\right\} = \left\{(q^n - 1) + \frac{q^r - b}{q^r}\right\} = \left\{\frac{q^r - b}{q^r}\right\} = \frac{q^r - (b \mod q^r)}{q^r} \tag{2}$$

and

$$\left\{\frac{b}{q^r}\right\} = \frac{b \mod q^r}{q^r} \tag{3}$$

From Lemma 4,

$$SBT\_path((q^r - x)/q^r) = \text{ exchange L and R in } SBT\_path(x/q^r).$$

Then, the length of $SBT\_path(x/q^r)$ and $SBT\_path((q^r - x)/q^r)$ coincide. Using (2) and (3) we conclude that the lengths of $SBT\_path(\{b/q^r\})$ and $(SBT\_path(\{(q^m - b)/q^r\})$ coincide. $\square$

Lemma 6. *Let q and m be positive integeres. Then for each positive integer a such that $a < q^m$ and a is coprime with q there is a positive integer a' such that*

$$SBT\_path(a'/q^m) = \textit{ reverse } SBT\_path(a/q^m)$$

and for every $r \in \{1, \ldots, m\}$ the lengths of $SBT\_path(\{a'/q^r\})$ and $SBT\_path(\{a/q^r\})$ coincide.

Proof. By Lemma 4, we know that for every s, t, *reverse* $SBT\_path(s/t) = SBT\_path(s'/t)$ for some positive integer s'.

From Lemma 3 we can write the matrix M_r that represents $\{a/q^r\} = a_r/q^r$

$$M_r = \begin{pmatrix} \frac{a_r(q^r - d_r)+1}{q^r} & \frac{a_r d_r - 1}{q^r} \\ q^r - d_r & d_r \end{pmatrix}$$

and $a_r d_r \equiv 1 \pmod{q^r}$.

By Lemma 4, we know that $d_m = a'$. Thus, $a_m a' \equiv 1 \pmod{q^m}$. By definition of a_r we have $a_r \equiv a_m \pmod{q^r}$. Then $a_r d_r \equiv a_m d_r \equiv 1 \pmod{q^r}$. Hence,

$$d_r = a' \mod q^r.$$

Also by Lemma 4 *reverse* $SBT\_path(\{a'/q^r\})$ and M_r, represent the same node in the Half-Stern-Brocot tree. Then, $SBT\_path(a_r/q^r)$ and $SBT\_path(\{a'/q^r\})$ have the same length for every $r \in \{1, \ldots, m\}$. $\square$

3.3 Proof of Theorem 1

Let $SBT\_path(b/q^m)$ denote the path in the Half-Stern-Brocot tree from the root to b/q^m. We define $b^{(2)}$, $b^{(3)}$, $b^{(4)}$, $a^{(2)}$, $a^{(3)}$, $a^{(4)}$ to the integers such that

$$SBT\_path(b^{(2)}/a^{(2)}) = \text{exchange L and R in } SBT\_path(b/q^m).$$
$$SBT\_path(b^{(3)}/a^{(3)}) = \text{reverse } SBT\_path(b/q^m).$$
$$SBT\_path(b^{(4)}/a^{(4)}) = \text{reverse } SBT\_path(b^{(2)}/a^{(2)}).$$

From Lemma 4 we know that

$$a^{(2)} = a^{(3)} = a^{(4)} = q^m,$$

$$b^{(2)} = q^m - b \quad \text{and} \quad b^{(4)} = q^m - b^{(3)}.$$

From Lemmas 4 and 3 we know that $b^{(3)} b \equiv 1 \pmod{q^m}$. By Lemmas 5 and 6, for every $r \in \{1, \ldots, m\}$, the lengths of $SBT\_path(\{b/q^r\})$, $SBT\_path(\{b^{(2)}/q^r\})$, $SBT\_path(\{b^{(3)}/q^r\})$ and $SBT\_path(\{b^{(4)}/q^r\})$ coincide. $\square$

4 A conjecture on the discrepancy of $(\{q^n\alpha\})_{n\geq 1})$

In [11, Theorem 1], given an integer q greater than or equal to 2, Levin proves that the number α

$$\alpha = \sum_{m\geq 1} \frac{1}{q^{n_m}} \sum_{k=0}^{q^m-1} \left\{ \frac{b_m k}{q^m} \right\} \frac{1}{q^{mk}}$$

$$\textit{where } n_1 = 0 \textit{ and } n_k = \sum_{r=1}^{k-1} rq^r, \textit{ for } k = 2, 3, \ldots$$

satisfies that $D_N(\{q^n\alpha\})_{n\geq 1})$ is in $O\big((\log N)^3/N\big)$. We conjecture that, in case α is defined using a sequence $(b_m)_{m\geq 1}$ where each b_m is a minimizer for (q, m), $D_N(\{q^n\alpha\})_{n\geq 1})$ is in $O\big((\log N)^2/N\big)$.

Supported by our experimental results we pose the following conjecture.

Conjecture 1. *For every positive integer q greater than or equal to 2 and for every positive m, each minimizer b_m for (q, m) satisfies*

$$\sum_{r=1}^{m} S(b_m/q^r) \leq qm^2.$$

The relevance of the conjecture is the following result.

Proposition 7. *Let q be an integer greater than or equal to 2. If $(b_m)_{m\geq 1}$ is such that each b_m is a minimizer for (q, m), and for each $m = 1, 2, \ldots$*

$$\sum_{r=1}^{m} S(b_m/q^r) \leq qm^2.$$

Then the number

$$\alpha = \sum_{m\geq 1} \frac{1}{q^{n_m}} \sum_{k=0}^{q^m-1} \left\{ \frac{b_m k}{q^m} \right\} \frac{1}{q^{mk}}$$

where $n_1 = 0$ and $n_k = \sum_{r=1}^{k-1} rq^r$, for $k = 2, 3, \ldots$, is normal to base q and $D_N((\{\alpha q^n\})_{n\geq 0}) = O\left((\log N)^2/N\right)$.

Before giving the proof of Proposition 7 we need some lemmas, that follow almost verbatim those given by Levin in [11, Theorem 1]. The following well known result gives the relation between the discrepancy estimates and the sum of partial quotients of continued fractions.

Lemma 8 (Theorem 3.3 [12], also Lemma 2 [11])**.** *Let q be a positive integer greater than or equal to 2. Let $j \geq 1$, let N be such that $1 \leq N \leq q^j$, and let b coprime with q. Let $S(x) = \sum_{i\geq 1} a_i(x)$. Then,*

$$ND_N(\{bn/q^j\})_{n\geq 0}) \leq S(b/q^j)$$

Let N be an integer in $[1, mq^m]$ and let a real number $\gamma \in (0, 1]$. We define

$$A(\gamma, N, (x_n)_{n\geq 0}) = \#\{n : 0 \leq n < N, \{x_n\} < \gamma\}$$
$$A(\gamma, P, Q, (x_n)_{n\geq 0}) = \#\{n : P \leq n < Q + P, \{x_n\} < \gamma\}$$

For $m \geq 1, b, i$ integers, $0 \leq i < m$, and b, q coprime, we define

$$\alpha_m = \alpha_m(b) = \sum_{k=0}^{q^m-1} \left\{ \frac{bk}{q^m} \right\} \frac{1}{q^{mk}}. \tag{4}$$

Lemma 9 (Lemma 1 [11])**.** *For $N \in [1, mq^m]$ be an integer, $\gamma \in (0,1]$ and b coprime with q. Then,*

$$A(\gamma, N, \{\alpha_m q^n\}_{n\geq 0}) = \gamma N + \varepsilon_1 \left(4m + 3\sum_{i=1}^{m} \max_{1\leq N\leq q^i} N D_N(\{bn/q^i\}_{n\geq 0})\right),$$
$$A(\gamma, mq^m, \{\alpha_m q^n\}_{n\geq 0}) = \gamma m q^m + 3\varepsilon_2 m,$$

with $|\varepsilon_j| < 1$, $j = 1, 2$.

Corollary 10. *Let $1 \leq N \leq mq^m$. Then $A(\gamma, N, \{\alpha_m(b_m)q^n\}_{n\geq 0}) = \gamma N + O(m^2)$.*

The statement follows from (4), Lemmas 8, 9 and from the hypothesis in Proposition 7.
By the definition of α and (4),

$$\left\{\alpha q^{n_m+n}\right\} = \{\alpha_m(b_m)q^n\} + \theta q^{n-mq^m} \textit{ with } 0 < \theta < 1 \textit{ and } 0 \leq n < mq^m.$$

Hence, for N in $[1, mq^m]$,

$$\begin{aligned} A(\gamma - 1/q^m, N-m, \{\alpha_m(b_m)q^n\}_{n\geq 0}) &\leq A(\gamma, N, \left\{\alpha q^{n_m+n}\right\}_{n\geq 0}) \\ &\leq A(\gamma, N, \{\alpha_m(b_m)q^n\}_{n\geq 0}) \end{aligned}$$

By Corollary 10, we obtain

$$A(\gamma, n_m, N, \{\alpha q^n\}_{n\geq 0}) = \gamma N + O(m^2) \textit{ with } 1 \leq N \leq mq^m. \tag{5}$$

Similarly, from Lemma 9,

$$A(\gamma, n_m, mq^m, \{\alpha q^n\}_{n\geq 0}) = \gamma m q^m + O(m). \tag{6}$$

Proof of Proposition 7. Assume the hypothesis is true. For every $N \geq 1$ there exists an integer k such that N in $[n_k, n_{k+1}]$.

$$N = n_k + R \qquad \textit{with } 0 \leq R < kq^k,\ (k-1)q^{k-1} < N,\ k \leq 2\log_q N. \tag{7}$$

Applying (5)-(7) we obtain

$$\begin{aligned} A(\gamma, N, \{\alpha q^n\}_{n\geq 0}) &= \sum_{r=1}^{k-1} A(\gamma, n_r, rq^r, \{\alpha q^n\}_{n\geq 0}) + A(\gamma, n_k, R, \{\alpha q^n\}_{n\geq 0}) \\ &= \sum_{r=1}^{k-1} (\gamma r q^r + O(r)) + \gamma R + O(k^2) \\ &= \gamma N + O(k^2) \\ &= \gamma N + O(\log^2 N). \end{aligned}$$

Thus, α is normal and $D_N((\{\alpha q^n\})_{n\geq 0}) = O\left((\log N)^2/N\right)$. □

The above proof shows that, indeed, if $\sum_{r=1}^{m} S(b_m/q^r) \leq f(m)$ for some integer function then $D_N((\{\alpha q^n\})_{n\geq 0})$ is $O(f(\log N)/N)$.

Appendix: Examples of minimizers

Tables 2, 3 and 4 exhibit minimizers for $q = 2, 3$ and 10.

m	b	$b^{(2)}$	$b^{(3)}$	$b^{(4)}$	has more
1	1	1	1	1	
2	1	3	1	3	
3	3	5	3	5	
4	3	13	11	5	
5	5	27	13	19	
6	19	45	27	37	
7	37	91	45	83	
8	45	211	165	91	
9	151	361	295	217	
10	151	873	807	217	
11	807	1241	1175	873	
12	867	3229	1611	2485	
13	3367	4825	4759	3433	
14	3433	12951	4825	11559	
15	4825	27943	19817	12951	True
16	13893	51643	27789	37747	True
17	51351	79721	79655	51417	
18	79655	182489	182423	79721	
19	79655	444633	444567	79721	
20	444567	604009	603943	444633	
21	444567	1652585	1652519	444633	
22	444567	3749737	3749671	444633	
23	1493143	6895465	6895399	1493209	
24	6895399	9881817	9881751	6895465	
25	6895465	26658967	9881817	23672615	
26	6895465	60213399	9881817	57227047	
27	9881817	124335911	74004329	60213399	
28	74004329	194431127	144099545	124335911	
29	74004329	462866583	412535001	124335911	
30	219756393	853985431	451332313	622409511	
31	219756393	1927727255	1525074137	622409511	
32	1525074137	2769893159	2367240041	1927727255	
33	2333453933	6256480659	6099667813	2490266779	
34	2333453933	14846415251	6099667813	11080201371	
35	2333453933	32026284435	6099667813	28260070555	
36	6099667813	36693192301	32026284435	62619808923	
37	32026284435	74819144549	62619808923	105412669037	
38	62619808923	169465237907	105412669037	212258098021	
39	169465237907	337497715867	212258098021	380290575981	

Table 2: Minimizers for $q = 2$.

m	b	$b^{(2)}$	$b^{(3)}$	$b^{(4)}$	has more
1	1	2	1	2	
2	2	7	5	4	
3	5	22	11	16	
4	31	50	34	47	
5	92	151	140	103	
6	140	589	578	151	True
7	857	1330	860	1327	
8	2570	3991	3980	2581	
9	9131	10552	10541	9142	
10	12262	46787	42883	16166	
11	31907	145240	68306	108841	
12	46787	484654	311411	220030	
13	311411	1282912	1109669	484654	True
14	1288610	3494359	1719647	3063322	
15	3761986	10586921	3794110	10554797	
16	7547866	35498855	30542071	12504650	
17	30041471	99098692	94985393	34154770	True

Table 3: Minimizers for $q = 3$

m	b	$b^{(2)}$	$b^{(3)}$	$b^{(4)}$	has more
1	3	7	7	3	
2	27	73	63	37	
3	173	827	237	763	True
4	2627	7373	3563	6437	True
5	22627	77373	43563	56437	
6	262113	737887	262177	737823	True
7	2262113	7737887	2262177	7737823	
8	16172177	83827823	65472113	34527887	True
9	226542279	773457721	742147319	257852681	

Table 4: Minimizers for $q = 10$

Code

```
#Sum continued fraction expansion
def S(numerator, denominator):
    if (denominator == 0):
        return 0
    return (numerator // denominator + S(denominator, numerator%denominator))

def get_one_bm(q, max_m):
    best_b_m, best_sum_S = [0] * max_m, [float('inf')] * max_m
    for candidate_bm in range(q ** max_m):
        if math.gcd(candidate_bm, q) == 1:
            sum_S_candidate = 0
            for r in range(1, max_m):
                sum_S_candidate += S(candidate_bm % q ** r, q ** r)
                if sum_S_candidate < best_sum_S[r]:
                    best_b_m[r], best_sum_S[r] = candidate_bm, sum_S_candidate
    return best_b_m

def get_alpha(q, b_m):
    alpha = ""
    for m in range(1,len(b_m)):
        for k in range(0, q ** m):
            alpha += numpy.base_repr((b_m[m]*k) % (q ** m), base=q).zfill(m)
    return alpha
alpha = get_alpha(q, get_one_bm(q, max_m))
```

Figure 3: Code to compute the number α using the smaller b_m that minimize (m, q).

Alpha as an image

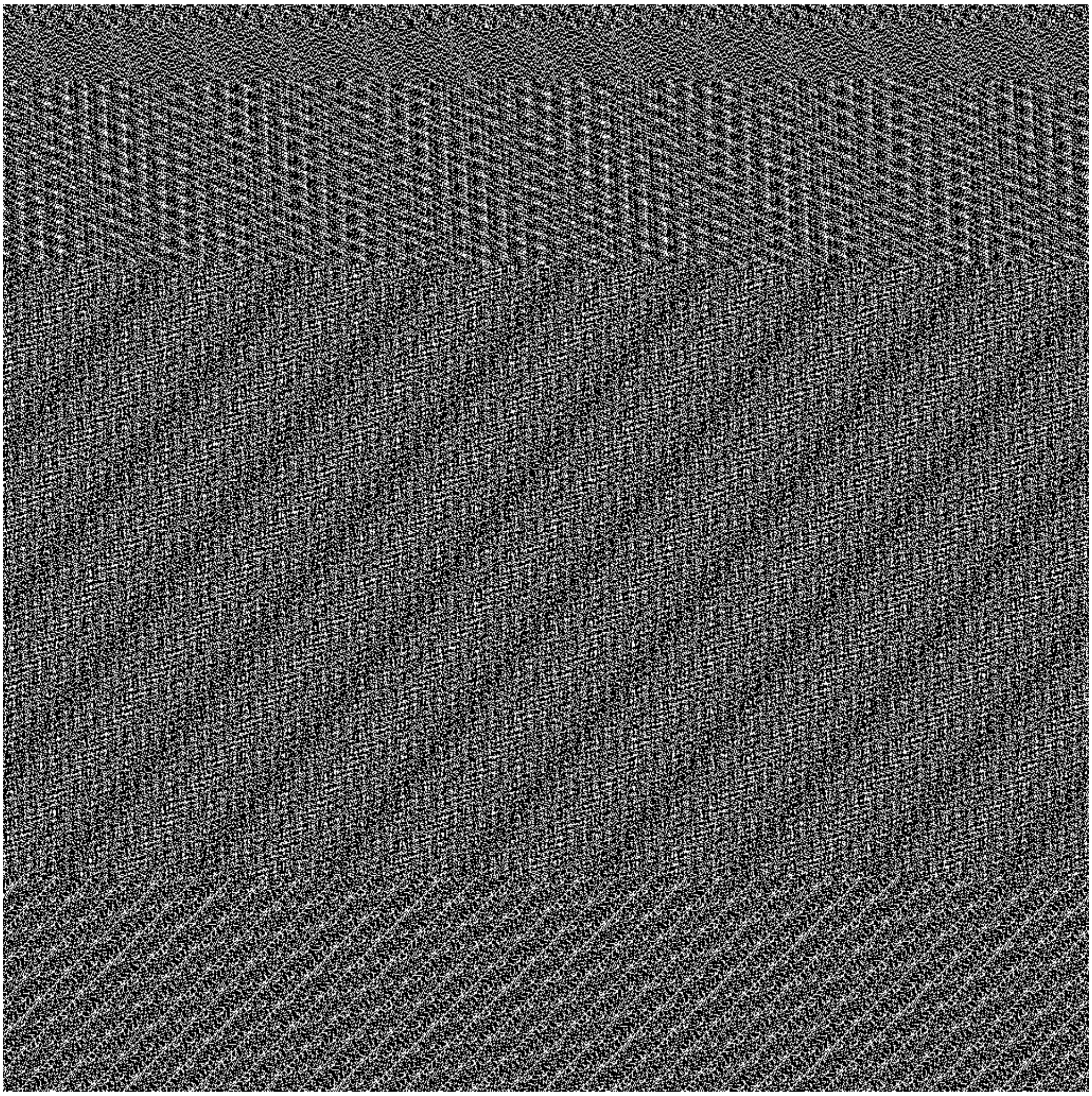

Figure 4: Using the result of the code before with $q = 2$, this image plots the first 2^{20} digits, where white pixels are 0s and black pixels are 1s.

References

[1] V. Becher and O. Carton. Normal numbers and nested perfect necklaces. *Journal of Complexity*, 54:in press, 2019.

[2] É. Borel. Les probabilités d'enombrables et leurs applications arithmétiques. *Supplemento di Rendiconti del Circolo Matematico di Palermo*, 27:247–271, 1909.

[3] Jean-Paul Allouche Boris Adamczewskia. Reversals and palindromes in continued fractions. *Theoretical Computer Science*, 380:220–237, 2007.

[4] Y. Bugeaud. *Distribution modulo one and Diophantine approximation*, volume 193 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2012.

[5] M. Drmota and R. Tichy. *Sequences, Discrepancies and Applications*. Lecture Notes in Mathematics, Vol. 1651. Springer-Verlag, 1997.

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

[7] 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.

[8] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics: A Foundation for Computer Science*. Addison-Wesley, second edition edition, 1994.

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

[10] L. Kuipers and H. Niederreiter. *Uniform distribution of sequences*. Dover Publications, Inc., New York, 2006.

[11] M. B. Levin. On the discrepancy estimate of normal numbers. *Acta Arithmetica*, 88(2):99–111, 1999.

[12] Harald Niedereiter. *Random Number Generation and Quasi Monte Carlo Methods*. Society for Industrial and Applied Mathematics, 1992.

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

[14] V. N. Popov. Asymptotic formula for the sum of sums of the elements of the continued fractions for numbers of the form a/p. *J. Soviet Math.*, 17, 1981.

[15] George N. Raney. On continued fractions and finite automata. *Mathematische Annalen*, 17:265–283, 1972.

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