NORMAL NUMBERS AND NESTED PERFECT NECKLACES

VERÓNICA BECHER AND OLIVIER CARTON

Abstract. M. B. Levin used Sobol-Faure low discrepancy sequences with Pascal traingle matrices modulo 2 to construct, a real number x such that the first N terms of the sequence $(2^n x \mod 1)_{n\geq 1}$ have discrepancy $O((\log N)^2/N)$. This is the lowest discrepancy known for this kind of sequences. In this note we characterize Levin's construction in terms of nested perfect necklaces, which are a variant of the classical de Bruijn sequences. Moreover, we show that every real number x whose binary expansion is the concatenation of nested perfect necklaces of exponentially increasing order satisfies that the first N terms of $(2^n x \mod 1)_{n\geq 1}$ have discrepancy $O((\log N)^2/N)$. For the order being a power of 2, we give the exact number of nested perfect necklaces and an explicit method based on matrices to construct each of them. The computation of the n-th digit of the binary expansion of a real number built from nested perfect necklaces requires $O(\log n)$ elementary mathematical operations.

Mathematics Subject Classification: 68R15, 11K16, 11K38

1. Introduction and statement of results

A real number x is normal to an integer base b if every block of digits in $\{0, \ldots, b-1\}$, of the same length, occurs in the base b expansion of x with the same limit frequency. Borel [2, 3] gave this definition more than 100 years ago and nowadays it is considered the most basic property of randomness for real numbers. A longstanding open question on normal numbers is what is the maximum achievable speed of convergence to normality [9]. The best result in this direction is due to M. B. Levin [12] who exhibited, a construction of the binary expansion of a number with the best known speed of convergence to normality. Either this speed is already the maximum or, necessarily, it is within a logarithmic factor of the absolute maximum due to a result of Schmidt [14].

In this note we give two results. The first, Theorem 1, is a characterization of Levin's construction in terms of a variant of classical de Bruijn sequences [4], that we call *nested perfect necklaces*. Moreover, every real number x whose binary expansion is the concatenation of nested perfect necklaces of exponentially increasing order has the same speed of convergence to normality as that obtained by Levin's construction [12]. Our second result, Theorem 2, gives the exact number of nested perfect necklaces of a given order and a method to construct each of them. This method is based on variants of Pascal triangle matrices modulo 2. Hence, the computation of the n-th digit of the binary expansion of a real number built from nested perfect necklaces requires $O(\log n)$ elementary mathematical operations.

The notion of speed of convergence to normality is formalized in the theory of uniform distribution modulo 1. For a sequence $(x_n)_{n\geq 0}$ of real numbers in the unit

Date: January 19, 2019.

interval the discrepancy of the first N elements is

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

In [14] Schmidt showed 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 is an optimal order of discrepancy since this lower bound is achieved by van der Corput sequences, see [10, 5, 3].

The property of Borel normality for real numbers can be defined in terms of uniform distribution. A sequence $(x_n)_{n\geq 0}$ of real numbers in the unit interval is uniformly distributed exactly when $\lim_{N\to\infty} D_N((x_n)_{n\geq 0}) = 0$. We write $\{x\}$ to denote $x - \lfloor x \rfloor$, the fractional part of x. For an integer b greater than 1, a real number x is normal to base b if and only if the sequence $(\{b^n x\})_{n\geq 0}$, is uniformly distributed in the unit interval. As said above, it is still unknown whether the optimal order of discrepancy can be achieved by a sequence of the form $(\{b^n x\})_{n\geq 0}$ for some real number x [9, 5, 3]. The lowest discrepancy known for sequences of this form is $O((\log N)^2/N)$ and it holds for a real number x constructed by Levin in [12, Theorem 2]. In that paper he uses Sobol-Faure sequences with the Pascal triangle matrix modulo 2, see [11, 12, 6].

The known constructions of normal sequences based on classical de Bruijn sequences do not improve Levin's discrepancy bound: in [15] it is proved that for each such sequence x the discrepancy of $(\{b^n x\})_{n\geq 0}$ is $O(\sqrt{(\log\log N)/N})$, which is the same as that for almost all real numbers, see [8, 13, 7].

Here we characterize the construction given by Levin in [12, Theorem 2] in terms of combinatorics of words and with a refinement of the so called *perfect necklaces* introduced in [1]. Fix an alphabet A. A word is a finite sequence of symbols and a necklace, or circular word, is the equivalence class of a word under rotations. For positive integers k and m, we call a necklace (k, m)-perfect if each word of length k occurs in it exactly m times at positions which are different modulo m (for any convention on the starting point). The length of a (k, m)-perfect necklace is $m|A|^k$ where $|A|$ denotes the cardinality of the alphabet A. In this note we consider the modulus m being a power of 2.

Notice that for $m = 1$, the (k, m)-perfect necklaces are exactly the de Bruijn sequences of order k. For the binary alphabet the word 0011 is a $(1, 2)$-perfect necklace. Both words 00110110 and 00011011 are $(2, 2)$-perfect necklaces. The segments in Champernowne sequence which are the concatenation in lexicographic order of all words of length k is a (k, k)-perfect necklace. For instance the following word is a $(3, 3)$-perfect necklace (the spacing is just for the readers convenience),

000 001 010 011 100 101 110 111

More generally, every arithmetic sequence with difference coprime with the alphabet size yields a perfect necklace [1, Theorem 5].

A word w is a (k, m)-*nested perfect necklace* if for each integer $\ell = 1, 2, \ldots, k$, each block of w of length $m|A|^\ell$ starting at a position congruent to 1 modulo $m|A|^\ell$ is a (ℓ, m)-perfect necklace. An alternative recursive definition of nested perfect necklaces is as follows. A word w is a (k, m)-nested perfect necklace if, first, it is a (k, m)-perfect necklace; and, second, either $k = 1$ or whenever w is factorized $w = w_1 \cdots w_{|A|}$ with each word w_i of length $m|A|^{k-1}$, then each word w_i is a $(k - 1, m)$-nested perfect necklace.

Notice that each (k,m)-nested perfect necklace is not an equivalence class closed under rotations, but it is a single word, with a unique initial position. The word 00110110 is a $(2,2)$-nested perfect necklace because it is a $(2,2)$-perfect necklace and both words 0011 and 0110 are $(1,2)$-perfect necklaces. The four words

0000111101011010
0011110001101001
0001111001001011
0010110101111000

are $(2,4)$-nested perfect necklaces. Both the concatenation of the first two and the concatenation of the last two are $(3,4)$-nested perfect necklaces. The concatenation of all of them is a $(4,4)$-nested perfect necklace. The concatenation of all words of the same length in lexicographic order yields a perfect necklace that is not a nested perfect necklace.

The statement of our first result is as follows.

Theorem 1. *The binary expansion of the number x defined by Levin in* [12, Theorem 2] *using the Pascal triangle matrix modulo* 2 *is obtained as the concatenation of (m,m)-nested perfect necklaces for $m = 2^d$ with $d = 0, 1, 2, \ldots$. Conversely, for every number x whose binary expansion is the concatenation of (m,m)-nested perfect necklaces for $m = 2^d$ with $d = 0, 1, 2\ldots$, the discrepancy $D_N((\{b^n x\})_{n\geq 0})$ is $O((\log N)^2/N)$.*

The result of Theorem 1 holds for any base b that is a prime number, but we can not prove that it holds for arbitrary integer bases. Actually in [12, Theorem 2] Levin gives a construction of the base b expansion of a number that is normal to base b, for any abritrary base b, not just for base 2. For each integer $d = 0, 1, \ldots$ he considers Pascal triangle up to row $m = 2^d$, he completes it with 0s to square form and he takes the entries modulo 2. Then he defines a new matrix by taking these entries modulo b. We have not been able to prove that the considered submatrices of such a matrix have non-zero determinant, as required.

To see that the result of Theorem 1 holds for any base b that is a prime number consider for each integer $d = 0, 1, \ldots$, the Pascal triangle up to row $m = b^d$. Complete it with 0s to a square form, take it modulo b (instead of of modulo 2) and call it M_d. All the considered sub-matrices have determinant 1 before reducing modulo b. Therefore, they also have determinant 1 modulo b. A similar argument proves that every number x whose b-ary expansion is the concatenation of (m,m)-nested perfect necklaces for $m = b^d$ with $d = 0, 1, 2\ldots$ is such that the sequence ($b^n x$ mod 1) has the stated discrepancy bound. Unfortunately this argument fails when b is not prime (among the things that fail, the matrix M_d is not upper triangular anymore).

Now consider the field $\mathbb{F}_2$ with two elements. We introduce a family of 2^{m-1} matrices of dimension $m \times m$ over $\mathbb{F}_2$ obtained by rotating the columns of the Pascal triangle matrix modulo 2. We identify words of two symbols with vectors and, for each matrix M in this family, we construct a nested perfect necklace by concatenating the words of the form $Mw \oplus z$, where w ranges over all words over $\mathbb{F}_2$ of length m in lexicographic order, $\oplus$ is the addition of vectors and z is a fixed word over $\mathbb{F}_2$ of length m. Such a necklace is called an *affine necklace*. Our second result is as follows.

Theorem 2. *For each $m = 2^d$ with $d = 0, 1, 2, \ldots$ there are 2^{2m-1} binary (m,m)-nested perfect necklaces and they are exactly the affine necklaces.*

2. Affine necklaces

We consider transformations on words obtained as linear maps over the field $\mathbb{F}_2$ with two elements. We identify the words of length n over $\mathbb{F}_2$ with the column vectors of dimension $n \times 1$ over $\mathbb{F}_2$. More precisely, we always identify the word $a_1 \cdots a_n$ where $a_i \in \mathbb{F}_2$ with the column vector $(a_1, \dots, a_n)^t \in (\mathbb{F}_2)_{n\times 1}$ where ^{t} denotes transpose of vectors and matrices. Suppose $w_1, \dots, w_k$ is a sequence of words, each of them of length n and M is a $n\times n$-matrix over $\mathbb{F}_2$, we may consider the concatenation $(Mw_1)(Mw_2)\cdots(Mw_k)$. In this writing, the matrix M is multiplied with each word w_i considered as a column vector, and the resulting column vector is viewed again as a word of length n. Similarly, the component-wise sum of vectors in $\mathbb{F}_2$ is used directly on words of the same length. It is denoted by the symbol $\oplus$.

We assume that the alphabet is $\mathbb{F}_2 = \{0, 1\}$ and that the modulus m is always a power of 2, namely $m = 2^d$ for some non-negative integer d. We define a family of matrices that we will use to construct explicitly some nested perfect necklaces. We start by defining by induction on d an $m \times m$-matrix M_d for each $d \geq 0$ by

$$M_0 = (1) \quad \text{and} \quad M_{d+1} = \begin{pmatrix} M_d & M_d \\ 0 & M_d \end{pmatrix}.$$

The matrices M_1 and M_2 are then

$$M_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The matrix M_d is a variant of Pascal's triangle modulo 2 in sqaure form, we prove it in Lemma 3 below. This matrix is almost the one used by Levin in [12] because we have reversed the order of the columns. This definition of the matrix M_d allows us to identify words with column vectors, which is not the case in [12].

For every d, the matrix M_d is upper triangular, that is $(M_d)_{i,j} = 0$ for $1 \leq j < i \leq 2^d$. The following lemma states that the upper part of the matrix M_d is the beginning of the Pascal triangle modulo 2 also known as the Sierpiński triangle.

Lemma 3. *For all integers d, i, j such that $d \geq 0$ and $1 < i \leq 2^d$ and $1 \leq j < 2^d$, $(M_d)_{i,j} = (M_d)_{i-1,j} \oplus (M_d)_{i,j+1}$.*

Proof. The proof is carried out by induction on d. For $d = 0$, the result is trivially true because there are no such i and j. For $d = 1$, the result trivially holds. Suppose that the result holds for M_d and let i, j be integers such that $1 < i \leq 2^{d+1}$ and $1 \leq j < 2^{d+1}$. If $i \neq 2^d + 1$ and $j \neq 2^d$, the three entries $(M_{d+1})_{i,j}$, $(M_{d+1})_{i-1,j}$ and $(M_{d+1})_{i,j+1}$ lie in the same quarter of the matrix M_{d+1} and the result follows from the induction hypothesis. Otherwise, the result follows from the followings facts. For each integer $d \geq 1$, the entry $(M_d)_{i,j}$ is equal to 1 if either $i = 1$ or $j = 2^d$ (first row and last column) and it is equal to 0 if $i = 2^d$ or $j = 1$ (last row and first column) and $(M_d)_{1,1} = (M_d)_{2^d,2^d} = 1$ (intersection of the two previous cases). These facts are easily proved by induction on d. □

We now introduce a family of matrices obtained by applying some rotations to columns of the matrix M_d. Let σ be the function which maps each word $a_1 \cdots a_n$ to $a_n a_1 a_2 \cdots a_{n-1}$ obtained by moving the last symbol to the front. Since words over $\mathbb{F}_2$ are identified with column vectors, the function σ can also be applied to a column vector.

Let $n_1, \dots, n_m$ be a sequence of integers such that $n_m = 0$ and $n_{i+1} \leq n_i \leq n_{i+1} + 1$ for each integer $1 \leq i < m$. Let $C_1, \dots, C_m$ be the columns of M_d, that is, $M_d = (C_1, \dots, C_m)$. Define

$$M_d^{n_1,\dots,n_m} = \big(\sigma^{n_1}(C_1), \dots, \sigma^{n_m}(C_m)\big).$$

The following are the eight possible matrices $M_d^{n_1,\dots,n_m}$ for $d = 2$ and $m = 2^2$.

$$\begin{array}{cccc}
M_2^{0,0,0,0} & M_2^{1,0,0,0} & M_2^{1,1,0,0} & M_2^{2,1,0,0} \\
\begin{pmatrix}1&1&1&1\\0&1&0&1\\0&0&1&1\\0&0&0&1\end{pmatrix} &
\begin{pmatrix}0&1&1&1\\1&1&0&1\\0&0&1&1\\0&0&0&1\end{pmatrix} &
\begin{pmatrix}0&0&1&1\\1&1&0&1\\0&1&1&1\\0&0&0&1\end{pmatrix} &
\begin{pmatrix}0&0&1&1\\0&1&0&1\\1&1&1&1\\0&0&0&1\end{pmatrix} \\
M_2^{1,1,1,0} & M_2^{2,1,1,0} & M_2^{2,2,1,0} & M_2^{3,2,1,0} \\
\begin{pmatrix}0&0&0&1\\1&1&1&1\\0&1&0&1\\0&0&1&1\end{pmatrix} &
\begin{pmatrix}0&0&0&1\\0&1&1&1\\1&1&0&1\\0&0&1&1\end{pmatrix} &
\begin{pmatrix}0&0&0&1\\0&0&1&1\\1&1&0&1\\0&1&1&1\end{pmatrix} &
\begin{pmatrix}0&0&0&1\\0&0&1&1\\0&1&0&1\\1&1&1&1\end{pmatrix}
\end{array}$$

Let $m = 2^d$ for some $d \geq 0$ and let k be some integer such that $1 \leq k \leq m$. Let $w_1, \dots, w_{2^m}$ be the enumeration in lexicographic order of all words of length m over $\mathbb{F}_2$. Let z be a word over $\mathbb{F}_2$ of length m and let $w'_i = w_i \oplus z$ for $1 \leq i \leq 2^m$.

Let M be a matrix of the form $M_d^{n_1,\dots,n_m}$ as above. Then, the concatenation

$$(Mw'_1)(Mw'_2)\cdots(Mw'_{2^k})$$

is called an (k, m)-*affine* necklace. In the sequel we refer to this necklace as the (k, m)-affine necklace obtained from the matrix $M = M_d^{n_1,\dots,n_m}$ and the vector z. Note that setting $z' = Mz$ gives $Mw'_i = Mw_i \oplus z'$ which justifies the terminology. In Lemma 4 each possible matrix $M = M_d^{n_1,\dots,n_m}$ is proved to be invertible and therefore each vector z' is equal to Mz for some vector z.

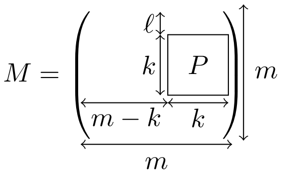

Figure 1. Position of the sub-matrix P in M in Lemma 4.

Lemma 4. *Let M be a matrix of the form $M_d^{n_1,\dots,n_m}$. Let ℓ and k be two integers such that $0 \leq \ell < \ell + k \leq 2^d$. The sub-matrix obtained by selecting the k rows $\ell + 1, \ell + 2, \dots, \ell + k$ and the last k columns $2^d - k + 1, \dots, 2^d$ of M is invertible.*

Note that for $k = 2^d$ and $\ell = 0$, the sub-matrix in the statement of the lemma, is the whole matrix $M_d^{n_1,\dots,n_m}$, which is invertible.

Proof. Let $m = 2^d$ be the number of rows and columns of M. By Lemma 3, each entry $M_{i,j}$ for $1 < i \leq m$ and $1 \leq j < m$ of the matrix M satisfies either $M_{i,j} = M_{i-1,j} \oplus M_{i,j+1}$ if $n_j = n_{j+1}$ (the column C_j has been rotated as much as the column C_{j+1}) or $M_{i,j} = M_{i-1,j} \oplus M_{i-1,j+1}$ if $n_j = n_{j+1} + 1$ (the column C_j has been rotated once more than the column C_{j+1}).

Let P be the sub-matrix in the statement of the lemma as shown in Figure 1. To prove that P is invertible we apply transformations to make it triangular. Note that all entries of the last column are 1. The first transformation applied to P is as follows. The row L_1 is left unchanged and the row L_i for $2 \leq i \leq k$ is replaced by $L_i \oplus L_{i-1}$. All entries of the last column but its top most one become zero. Furthermore, each entry is $P_{i,j}$ is replaced by either $P_{i,j+1}$ or $P_{i-1,j+1}$ depending on the value $n_j - n_{j+1}$. Note also that the new values of the entries still satisfy either $P_{i,j} = P_{i-1,j} \oplus P_{i,j+1}$ or $P_{i,j} = P_{i-1,j} \oplus P_{i-1,j+1}$ depending on the value $n_j - n_{j+1}$. The second transformation applied to P is as follows. The rows L_1 and L_2 are left unchanged and each row L_i for $3 \leq i \leq k$ is replaced by $L_i \oplus L_{i-1}$. All entries of the second to last column but its two topmost ones are now zero. At step n for $1 \leq n < k$, rows $L_1, \ldots, L_n$ are left unchanged and each row L_i for $n+1 \leq i \leq k$ is replaced by $L_i \oplus L_{i-1}$. After applying all these transformations for $1 \leq n < k$, each entry $P_{i,j}$ for $i+j = k+1$ satisfies $P_{i,j} = 1$ and each entry $P_{i,j}$ for $i+j > k+1$ satisfies $P_{i,j} = 0$. It follows that the determinant of P is 1 and that the matrix P is invertible. □

3. Affine necklaces are nested perfect necklaces

We introduce the notions of *upper* and *lower border* of a matrix $M_d^{n_1,\ldots,n_m}$. Let $m = 2^d$ for some $d \geq 0$ and let M be one matrix $M_d^{n_1,\ldots,n_m}$. An entry $M_{i,j}$ for $1 \leq i, j \leq m$ is said to be in the *upper border* (respectively *lower border*) of M if $M_{i,j} = 1$ and $M_{k,j} = 0$ for all $k = 1, \ldots, i-1$ (respectively for all $k = i+1, \ldots, m$). For instance, the upper border of the matrix $M_d^{0,\ldots,0} = M_d$ is the first row and its lower border is the main diagonal. The following pictures in boldface the upper and lower borders of the matrix $M_3^{3,3,2,1,1,1,0,0}$:

$$M_3^{3,3,2,1,1,1,0,0} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} \\ 0 & 0 & 0 & \mathbf{1} & \mathbf{1} & \mathbf{1} & 0 & 1 \\ 0 & 0 & \mathbf{1} & 1 & 0 & 1 & 1 & 1 \\ \mathbf{1} & \mathbf{1} & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & \mathbf{1} & \mathbf{1} & \mathbf{1} & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \end{pmatrix}$$

We gather now some easy facts about the upper and lower borders of a matrix $M_d^{n_1,\ldots,n_m}$. Both borders start in the unique entry 1 of the first column. The upper border ends in the top most entry of the last column and the lower border ends in the bottom most entry of the last column. The upper border only uses either East or North-East steps and the lower border only uses either East or South-East steps. The upper border uses a East step from column C_j to column C_{j+1} if $n_j = n_{j+1}$ and uses a North-East step if $n_j = n_{j+1} + 1$. Furthermore, whenever the upper border uses an East (respectively North-East) step to go from one columns to its right neighbour, the lower border uses a South-East (respectively East) step. This is due to the fact that the distance from the upper border to the lower border in the i-th column is $i - 1$.

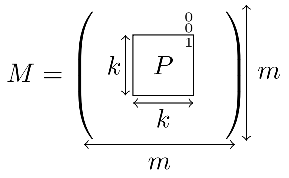

Figure 2. Position of the sub-matrix P in M in Lemma 5

Due to the symmetry in the matrix $M_d^{0,\dots,0} + M_d$ Lemma 4 applies also to the sub-matrices of $M_d^{0,\dots,0}$ obtained by selecting the first row. Since this symmetry is lost for the other matrices $M_d^{n_1,\dots,n_m}$, we need the following lemma which accounts for the rotations made to the columns in $M_d^{0,\dots,0}$ to obtain $M_d^{n_1,\dots,n_m}$.

Lemma 5. *Let M be a matrix of the form $M_d^{n_1,\dots,n_m}$. Let k be an integer such that $1 \le k \le 2^d$. The $k \times k$-sub-matrix obtained by selecting k consecutive rows and k consecutive columns in such a way that its top right entry lies on the upper border of M is invertible.*

Proof. The proof is similar to that of Lemma 4. Let P be the sub-matrix in the statement of the lemma, a picture appears in Figure 2. We apply transformations to the sub-matrix P to put it in a nice form such that the determinant is easy to compute. Just to fix notation, we suppose that the sub-matrix P is obtained by selecting rows $L_{r+1},\dots,L_{r+k}$ and columns $C_{s+1},\dots,C_{s+k}$. The hypothesis is that the entry $M_{r+k,s+k}$ is in the upper border of M. Note that the upper borders of M and P coincide inside P. We denote by $j_1,\dots,j_t$ the indices of the columns of P in $1,\dots,k$ which are reached by a North-East step of the upper border. This means that $j_1,\dots,j_t$ is the sequences of indices j such that $n_{s+j-1} = n_{s+j}+1$. By convention, we set $j_0 = 1$, that is, the index of the first column of P.

The first transformation applied to the matrix P is the following. The columns $C_1,\dots,C_{j_t-1}$ and C_k are left unchanged and each column C_j for $j_t \le j \le k-1$ is replaced by $C_j \oplus C_{j+1}$. All entries of the first row but its right most one become zero.

Furthermore, each entry $P_{i,j}$ for $j_t \le j \le k-1$ is replaced by $P_{i-1,j}$. The second transformation applied to the matrix P is the following. The columns $C_1,\dots,C_{j_{t-1}-1}$ and C_{k-1},C_k are left unchanged and each column C_j for $j_{t-1} \le j \le k-2$ is replaced by $C_j \oplus C_{j+1}$. The first row remains unchanged and all entries of the second row but the last two become 0. We apply t transformations like this one using successively $j_t, j_{t-1},\dots,j_1$. Then $k-t-1$ further steps are made using then $j_0 = 1$ each time. After applying all these transformations, each entry $P_{i,j}$ for $i+j = \ell+1$ satisfies $P_{i,j} = 1$ and each entry $P_{i,j}$ for $i+j < \ell+1$ satisfies $P_{i,j} = 0$. It follows that the determinant of P is 1 and that the matrix P is invertible. □

For a word w we write w^n to denote the word given by concatenation of n copies of w. The following lemma states that each (k,m)-nested perfect necklace can be transformed into another (k,m)-nested perfect necklace which starts with 0^m.

Lemma 6. *Let w be a word of length $m2^k$ and let z be a word of length m. The word w is a (k,m)-nested perfect necklace if and only if the word $w \oplus z^{2^k}$ is a (k,m)-nested perfect necklace.*

Proof. Note first that both words w and z^{2^k} have a length of $m2^k$. Let w' be the word $w \oplus z^{2^k}$. Let ℓ be an integer such that $1 \le \ell \le k$ and let v' be a block of w' of length $m2^\ell$ starting at a position j congruent to 1 modulo $m2^\ell$. The corresponding block of w at the same position j is of course $v = v' \oplus z^{2^\ell}$. By hypothesis, this later block v is a (ℓ,m)-nested perfect necklace. We claim that v' is also a (ℓ,m)-nested perfect necklace.

Let i be such that $1 \le i \le m$ and let u' any word of length ℓ. Let t be the block of zz of length ℓ starting at position i and consider the word $u = u' \oplus t$. This word u has an occurrence in the necklace v at a position j' congruent to i modulo m. It follows that $u' = u \oplus t$ has an occurrence at the same position j' in v'. Since each word u has such an occurrence for each possible i and v' has length $m2^\ell$, v' is a (ℓ,m)-nested perfect necklace. □

We can now prove that the all the (k,m)-affine necklaces are (k,m)-nested perfect necklaces.

Proposition 7. *Let k, m, d be integers such that $d \geq 0$, $m = 2^d$ and $1 \leq k \leq m$. Each (k,m)-affine necklace is a (k,m)-nested perfect necklace.*

The proof of Proposition 7 follows and extends that of [12, Lemma 5] but we use a different notation.

Proof. It suffices of course to prove the result for $k = m$. By Lemma 6, it may be assumed that the vector z in the definition of affine necklaces is the zero vector. Let M be one of the matrices $M_d^{n_1,\ldots,n_m}$, let $w_1, \ldots, w_{2^m}$ be the enumeration in lexicographic order of all words of length m over $\mathbb{F}_2$ and suppose that the (m,m)-affine necklace w is the concatenation $(Mw_1)(Mw_2)\cdots(Mw_{2^m})$. Let k be an integer such that $1 \leq k \leq m$ and let w' be a block of w of length $m2^k$ starting at a position congruent to 1 modulo $m2^k$. The word w' is thus equal to a concatenation of the form $(Mw_{p2^k+1})\cdots(Mw_{(p+1)2^k})$ for some fixed integer p such that $0 \leq p \leq 2^{m-k} - 1$. We claim that w' is a (k,m)-perfect necklace.

To prove the claim, it must be shown that for each integer ℓ such that $0 \leq \ell < m$, each word u of length k has exactly one occurrence in w with a starting position congruent to $\ell + 1$ modulo m (we write $\ell + 1$ rather than ℓ because positions are numbered from 1). We suppose that the word u and the integer ℓ such that $0 \leq \ell < m$ are fixed. We distinguish two cases depending on whether $\ell + k \leq m$ or not.

We first suppose that $k + \ell \leq m$. It follows that the wanted occurrence of u must be fully contained in a single word Mw_{p2^k+q} for $1 \leq q \leq 2^k$. More precisely it must lie in the positions $\ell+1, \ldots, \ell+k$ of Mw_{p2^k+q}. In that case, the claim boils down to showing that there is exactly one integer q such that u occurs in positions $\ell+1, \ldots, \ell+k$ of Mw_{p2^k+q}. Let us recall that p is fixed and that q ranges in $1, \ldots, 2^k$. Since w_i is the base 2 expansion of $i-1$ with m bits, w_{p2^k+q} has a factorization of the form $x_p y_{q-1}$, where x_p and y_{q-1} are the base 2 expansions of p and $q-1$ with $m-k$ and k bits, respectively.

$$M = \begin{pmatrix} \\ \boxed{\quad N \quad} & \boxed{\; P \;} \\ \\ \end{pmatrix}$$

The occurrence of u in w_{p2^k+q} is now translated into linear equations by introducing the following two matrices N and P (see above). Let N and P be the following sub-matrices of the matrix M. The $k \times m-k$ matrix N is obtained by selecting the k rows $L_{\ell+1}, \ldots, L_{\ell+k}$ and the $m-k$ columns $C_1, \ldots, C_{m-k}$. The $k \times k$ matrix P is obtained by selecting the same k rows $L_{\ell+1}, \ldots, L_{\ell+k}$ and the k columns $C_{m-k+1}, \ldots, C_m$. The word u occurs in the positions $\ell+1, \ldots, \ell+k$ of Mw_{p2^k+q} if and only if $u = Nx_p + Py_{q-1}$ where words u, x_p and y_{q-1} are considered as columns vectors of respective dimensions k, $m-k$ and k. Since x_p is fixed and P is invertible by Lemma 4, there is exactly one solution for y_{q-1} and thus one solution for q. This proves the claim when $k + \ell \leq m$.

We suppose that $\ell + k > m$. The wanted occurrence of u must then overlap two consecutive words Mw_{p2^k+q} and Mw_{p2^k+q+1} where $p2^k+q+1$ should be understood as $p2^k+1$ if $q = 2^k$. Let us write $u = u_1u_2$ where u_1 and u_2 have length $m - \ell$ and $\ell + k - m$. The wanted occurrences exist if u_1 occurs at positions $\ell+1, \ldots, m$ of Mw_{p2^k+q} and u_2 occurs at positions $1, \ldots, \ell+k-m$ of Mw_{p2^k+q+1} with the same convention for $p2^k + q + 1$. As in the previous case, these occurrences are translated into linear equations. For that purpose, we introduce the following four matrices.

$$M = \begin{pmatrix} \boxed{N_2} & \boxed{P_2} \\ & \\ \boxed{N_1} & \boxed{P_1} \end{pmatrix}$$

The matrices N_1 and P_1 are obtained by selecting the rows $L_{\ell+1}, \dots, L_m$ and the columns $C_1, \dots, C_{m-k}$ for N_1 and $C_{m-k+1}, \dots, C_m$ for P_1. The matrices N_2 and P_2 are obtained by selecting the rows $L_1, \dots, L_{\ell+k-m}$ and the columns $C_1, \dots, C_{m-k}$ for N_2 and $C_{m-k+1}, \dots, C_m$ for P_2 (see above). The two words w_{p2^k+q} and w_{p2^k+q+1} are then factorized $w_{p2^k+q} = x_p y_{q-1}$ and $w_{p2^k+q+1} = x_p y_q$ where x_p is the base 2 expansion of p with 2^{m-k} bits and words y_{q-1} and y_q are the base 2 expansions of $q-1$ and q (understood as 0 if $q = 2^k$) with 2^k bits. The occurrences of u_1 and u_2 do exist as wanted if and only if these two equalities hold,

$$\begin{aligned} u_1 &= N_1 x_p + P_1 y_{q-1}, \\ u_2 &= N_2 x_p + P_2 y_q \end{aligned}$$

Notice that the first equation involves y_{q-1} while the second one involves y_q. These two words are strongly related in the sense that each one determines the other. For each i such that $0 \leq i \leq k$, the i right most bits of either y_{q-1} or y_q determine the i right most bits of the other. This is due to the fact that either adding or subtracting 1 can be performed on the bits from right to left. For that reason, we will show that the equations $u_1 = N_1 x_p + P_1 y_{q-1}$ and $u_2 = N_2 x_p + P_2 y_q$ have a unique solution in q by successively computing the bits of $q-1$ and q from right to left.

We actually describe a strategy for solving the two equations. This strategy is based of the upper and lower borders of the matrix M. The main ingredient is that between two consecutive columns C_j and C_{j+1}, one of the two borders uses a step which is not horizontal, that is, either North-East for the upper border or South-East for the lower border.

The right most bit of y_{q-1} and y_q can be found as follows. Either the upper border or the lower border makes a non horizontal step from C_{m-1} to C_m. It means that either the first row or the last row of M has the form $(0, \dots, 0, 1)$. This row can be used to find the right most bit of y_{q-1} and y_q as it is the first row the equation $u_1 = N_1 x_p + P_1 y_{q-1}$ or the last row of the equation $u_2 = N_2 x_p + P_2 y_q$. The second right most bit of y_{q-1} and y_q can be found as follows. Either the upper border or the lower border makes a non horizontal step from C_{m-2} to C_{m-1}. It means that one row of M has the form $(0, \dots, 0, 1, *)$. It can be used to find the second right most bit of y_{q-1} and y_q as it is one row of one of the two equations.

This process can be continued using at each step a row of either the first or the second equation. In the process rows of the first equation are used from the first to the last while rows of the second equation are used from the last to the first. This process can be continued until the rows of one the equations have been exhausted. By symmetry, it can be assumed that all rows of the second equation have been used. Suppose that the left most n bits of y_{q-1} and y_q have still to be found. Then the last n rows of the first equations have not been used. Considering the known bits as constants, the matrix involving the r unknown bits is a matrix as in Lemma 5. By this lemma, this matrix is invertible and these last r bits can be found in a unique way. This proves the claim when $\ell + k > m$ and finishes the proof of the proposition. □

4. Nested perfect necklaces are affine necklaces

We show that all (k, m)-nested perfect necklaces are (k, m)-affine necklaces. Since the other inclusion has been already proved, it suffices to show that they have the same cardinality. The next lemma shows that for $k = 1$, they coincide.

Lemma 8. *The $(1, m)$-nested perfect necklaces are the words of the form ww' where w and w' are two words of length m satisfying $w' = w \oplus 1^m$. Furthermore, they are all affine.*

Proof. It is straightforward that $(1, m)$-nested perfect necklaces are the words of the form stated in the lemma. And for each matrix M of the form $M_d^{n_1,\ldots,n_m}$, Mw_0 and Mw_1 are respectively equal to 0^m and 1^m. This proves the last claim. □

The next lemma provides the number of (m, m)-affine necklaces. It shows that (m, m)-affine necklaces obtained by the different choices of the matrix $M_d^{n_1,\ldots,n_m}$ and of the vector z are indeed different.

Lemma 9. *Let $m = 2^d$ for some $d \geq 0$. There are exactly 2^{2m-1} different (m, m)-affine necklaces.*

Proof. There are exactly 2^{m-1} matrices $M_d^{n_1,\ldots,n_m}$. Indeed, the sequence $n_1, \ldots, n_m$ is fully determined by the sequence $n_1 - n_2, \ldots, n_{m-1} - n_m$ of $m - 1$ differences which take their value in $\{0, 1\}$. There are also 2^m possible values for the word z in $\mathbb{F}_2^m$. This proves that the number of (m, m)-affine necklaces is bounded by 2^{2m-1}.

It remains to show that two (m, m)-affine necklaces obtained for two different pairs (M, z) and (M', z') are indeed different. Let $w_1, \ldots, w_{2^d}$ be the enumeration in lexicographic order of all words of length m over $\mathbb{F}_2$. Let M and M' be two matrices of the form $M_d^{n_1,\ldots,n_m}$. Let z and z' be two words over $\mathbb{F}_2$ of length m and let $u_i = w_i \oplus z$ and $u'_i = w_i \oplus z'$ for $1 \leq i \leq 2^m$. Let w and w' be the two concatenations $(Mu_1) \cdots (Mu_{2^d})$ and $(M'u'_1) \cdots (M'u'_{2^d})$. We claim that if $w = w'$, then $M = M'$ and $z = z'$.

We suppose that $w = w'$. Since both matrices M and M' are invertible by Lemma 4, Mu_i (respectively $M'u'_i$) is the zero vector if and only if u_i (respectively u'_i) is the zero vector, that is, $z = w_i$ (respectively $z' = w_i$). It follows then that $z = z'$ and thus $u_i = u'_i$ for $1 \leq i \leq 2^m$. Note that the vector u_i ranges over all possible vectors of length m. If $Mu_i = M'u_i$ for all $1 \leq i \leq 2^m$, then $M = M'$. □

Lemma 12 will show how (k, m)-affine necklaces can be concatenated with (k, m)-affine necklaces to get $(k + 1, m)$-perfect necklaces. The next two lemmas are intermediate steps towards the proof. The first states that each rotation of a column of M_d is a linear combination of some columns to its right.

Lemma 10. *Let $d \geq 0$ be integer and let $(C_1, \ldots, C_{2^d})$ be the columns of the matrix M_d. For any integers i, k such that $1 \leq i \leq 2^d$ and $k \geq 0$, the vector $\sigma^k(C_i) \oplus C_i$ is equal to a linear combination $\bigoplus_{j=i+1}^{2^d} b_j C_j$ where $b_j \in \mathbb{F}_2$.*

Proof. The result is proved by the induction on the difference $2^d - i$. If $i = 2^d$, the result holds trivially because $\sigma(C_{2^d}) = C_{2^d}$. Assume that $i < 2^d$ is fixed. The proof is now by induction on the integer k. The result for $k = 0$ is trivially true. By Lemma 3 applied to the column C_{i+2^d} of the matrix M_{d+1}, the equality $\sigma(C_i) \oplus C_i = C_{i+1}$ holds. We apply Lemma 3 to the column C_{i+2^d} of the matrix M_{d+1} because this column has period 2^d and its first half is the column C_i of M_d. This proves the result for $k = 1$. Suppose now that the result is true for some $k \geq 1$. Applying σ to both terms of the equality and replacing first $\sigma(C_i)$ by the value $C_i \oplus C_{i+1}$ and second each $\sigma(C_j)$ by the value given by the induction hypothesis gives the result for $k + 1$. □

The next lemma shows for each (k,m)-affine necklace, there is just one possible way of rotating it to get another (k,m)-affine necklace.

Lemma 11. *Let d, m, k and p be integers such that $d \geq 0$, $m = 2^d$, $1 \leq k \leq m$ and $p \geq 0$. Let w be a (k,m)-affine necklace. If m divides p and $\sigma^p(w)$ is also a (k,m)-affine necklace, then $p \equiv m2^{k-1} \mod |w|$.*

Proof. Since $|w| = m2^k$ and $\sigma^{|w|}(w) = w$, we may assume that $0 \leq p \leq m2^k$. The result holds if either $p = 0$ or $p = m2^k$. Therefore we assume that $1 \leq p \leq m2^k - 1$. Let $w_1, \dots, w_{2^m}$ be the enumeration in lexicographic order of all words over $\mathbb{F}_2$ of length m. Since w is an affine necklace, it is a concatenation $(Mu_1) \cdots M(u_{2^k})$ where M is a matrix $M_d^{n_1,\dots,n_m}$ and u_i is equal to $w_i \oplus z$ for each integer $1 \leq i \leq 2^k$ and for some fixed vector z. Since $\sigma^p(w)$ is also an affine necklace, it is a concatenation $(M'u'_1) \cdots (M'u'_{2^k})$ where M' is a matrix $M_d^{n_1,\dots,n_m}$ and u'_i is equal to $w_i \oplus z'$ for each integer $1 \leq i \leq 2^k$ and for some other fixed vector z'. For each ℓ such that $0 \leq \ell < m$, consider the vector $M'u'_1 \oplus M'u'_{1+2^\ell}$. Since $u'_1 \oplus u'_{1+2^\ell} = w_1 \oplus w_{1+2^\ell}$ and since w_{1+2^ℓ} is the vector having a single 1 in position $m - \ell$, $M'u'_1 \oplus M'u'_{1+2^\ell}$ is equal to the column $C'_{m-\ell}$ of the matrix M'. Since M and M' are two matrices of the form $M_d^{n_1,\dots,n_m}$, the column $C'_{m-\ell}$ of M' is equal to $\sigma^t(C_{m-\ell})$ where $C_{m-\ell}$ is the corresponding column of M and t is some integer. Since m divides p, the necklace $\sigma^p(w)$ is also equal to

$$(Mu_i) \cdots (Mu_{2^k})(Mu_1) \cdots (Mu_{i-1})$$

where $i = 1 + p/m$. We consider the word w_i which is the base 2 expansion of $i - 1$ with m bits. Let ℓ be the greatest integer such that 2^ℓ divides $i - 1 = p/m$. The integer $i - 1$ is equal to $2^\ell(2r + 1)$ for some non-negative integer r. We claim that $\ell = k - 1$.

Suppose by contradiction that $\ell < k - 1$. The integer r satisfies thus $r \geq 0$ and the base 2 expansion of $2r+1$ is $u1$ where u the base 2 expansion of r. The word w_i is then equal to $0^{m-k}u10^\ell$ where 0^{m-k} is the block leading zeros due to $i \leq 2^k$ and u is the base 2 expansion of r with $k-\ell-1$ digits. We consider the word w_{i+2^ℓ}. This word is equal to $0^{m-k}u'0^{\ell+1}$ where u' is the base 2 expansion of $r+1$ with $k-\ell-1$ digits. Computing $Mu_i \oplus Mu_{i+2^\ell} = Mw_i \oplus Mw_{i+2^\ell}$ gives $C_{2^d-\ell} \oplus R$ where R is a non-zero linear combination of $C_{m-k}, \dots, C_{m-\ell-1}$. This linear combination R cannot be equal to zero because the words u and u' are different. The vector $Mu_i \oplus Mu_{i+2^\ell}$ is also equal to $M'u'_1 \oplus M'u'_{1+2^\ell} = C'_{m-\ell} = \sigma^t(C_{m-\ell})$. By Lemma 10, this vector is equal to $C_{m-\ell} \oplus R'$, where R' is a linear combination of $C_{m-\ell+1}, \dots, C_m$. This is a contradiction: the equality $R = R'$ is impossible because, by Lemma 4, the matrix M is invertible. □

We are now ready to show that each (k,m)-affine necklace can be extended by at most two (k,m)-affine necklaces to get a $(k+1,m)$-perfect necklace.

Lemma 12. *Let $m = 2^d$ for some $d \geq 0$ and let k be an integer such that $1 \leq k \leq m$. Let w be a (k,m)-affine necklace. There are at most two (k,m)-affine necklaces w' such that ww' is a $(k+1,m)$-perfect necklace.*

Proof. We use the characterization of (k,m)-perfect necklaces as cycles in appropriate graphs G_k (variants of de Bruijn graphs) given in [1]. Consider the directed graph G_k whose vertex set is $\mathbb{F}_2^k \times \{1, \dots, m\}$ and whose transitions are defined as follows. There is an edge in G_k from (u,i) to (u',i') if first there are two symbols a and b in $\mathbb{F}_2$ such that $ua = bu'$ and second $i' \equiv i + 1 \mod m$. The condition on u and u' means that u and u' are respectively the prefix and the suffix of length k of the word $v = ua = bu'$ of length $k + 1$. Therefore, the edges of the graph G_k can be identified with the words of length $k + 1$ over $\mathbb{F}_2$. Note that each vertex of G_k has two incoming and two outgoing edges. It follows from the definition of the graph G_k, that each (k,m)-nested perfect necklace can be interpreted as a Hamiltonian cycle in G_k and that each $(k+1,m)$-nested perfect necklace as an Eulerian cycle in G_k.

Let w be a (k,m)-affine necklace. Then w determines a Hamiltonian cycle C in G_k. Since C visits each node of G_k exactly once, it uses one outgoing edge of each node. Any (k,m)-nested perfect necklace w' such that ww' is a $(k+1,m)$-nested perfect necklace induces an Hamiltonian C' cycle which cannot use an edge of C. Otherwise, it would not be possible to build an Eulerian cycle from C and C' and ww' would not be a $(k+1,m)$-nested perfect necklace. If there is no (k,m)-affine necklace w' such that ww' is a $(k+1,m)$-nested perfect necklace the lemma trivially holds. Suppose now that there exists at least one such w'. Since the graph $G_k \setminus C$ has only one outgoing edge from any vertex, any (k,m)-nested perfect necklace w'' such that ww'' is a $(k+1,m)$-nested perfect necklace must be of the form $\sigma^p(w')$ for some integer $p \geq 0$. Since both Hamiltonian cycles C' and C'' induced by w' and w'' must start from a vertex in $\mathbb{F}_2^k \times \{1\}$ it follows that m divides p. By Lemma 11, the only possible choices for p are 0 and $m2^{k-1}$. This proves that there is at most one such w'' different from w'. □

We can now give the number of (k,m)-affine necklaces.

Proposition 13. *Let $m = 2^d$ for some $d \geq 0$. For each integer k such that $1 \leq k \leq m$, the number of (k,m)-affine necklaces is exactly 2^{k+m-1}.*

Proof. We assume the integer m to be fixed and we let t_k denote the number of (k,m)-affine necklaces. By Lemma 8, t_1 is equal to 2^m and by Lemma 9, t_m is equal to 2^{2m-1}. It follows from Lemma 12 that $t_{k+1} \leq 2t_k$ for each integer k such that $1 \leq k < m$. None of these inequalities can be strict because otherwise t_m would be striclty less that 2^{2m-1}. So, for each integer k such that $1 \leq k \leq m$, $t_{k+1} = 2t_k$, hence, $t_k = 2^{k+m-1}$. □

The results above allows us to prove the wanted inclusion.

Proposition 14. *Each (k,m)-nested perfect necklace is a (k,m)-affine necklace.*

Proof. Fix m, let s_k be the number of (k,m)-nested perfect necklaces and let t_k be the number of (k,m)-affine necklaces. By Proposition 7, $s_k \leq t_k$ holds for each integer k such that $1 \leq k \leq m$. To prove the statement, it suffices to prove that $s_k = t_k$ for each integer k such that $1 \leq k \leq m$. We prove it by induction on k. By Lemma 8, $s_1 = t_1 = 2^m$. We suppose $s_k = t_k$ and we prove that $s_{k+1} = t_{k+1}$. Each $(k+1,m)$-nested perfect necklace can be written as ww' where w and w' are two (k,m)-nested perfect necklaces. Since $s_k = t_k$, w and w' are also (k,m)-affine necklaces. By Lemma 12, there are at most two possible choices of w' for each w. This proves that $t_{k+1} \leq 2t_k$. Since $s_{k+1} = 2s_k$ by Proposition 13 and $s_{k+1} \leq t_{k+1}$, the equality $s_{k+1} = t_{k+1}$ holds. □

5. Proof of Theorems 1 and 2

5.1. **Proof of Theorem 1.** For each integer $d = 0,1,\ldots$ consider the Pascal triangle up to row $m = 2^d$. Complete it with 0s to obtain a square matrix and now take this matrix modulo 2. Notice that Levin's construction in [12, Theorem 2] is the concatenation of blocks obtained using this matrix for increasing $m = 2^d$ with $d = 0,1,2,\ldots$. Hence, each block of the constructed binary sequence is an (m,m)-affine necklace and, as we proved in Proposition 7, each block is an (m,m)-nested perfect necklace.

Conversely, assume that the binary expansion of a given real x can be split in consecutive blocks such that each block is an (m,m)-nested perfect necklace for $m = 2^d$ with $d = 0, 1, 2, \ldots$. In each (m, m)-nested perfect necklace, each block of length m occurs exactly m times at different positions modulo m. To bound the discrepancy of the sequence $(2^n x \mod 1)_{n\geq 1}$ at position N Levin bounds the error in a multiplicative way: for each block of length m he multiplies the number of possible congruence classes of a position (namely m) times the number of occurrences that the block can have in the positions in that congruence class. Thus, given a position N there are positive integers k and R such that $N = \sum_{d=1}^{k-1} 2^d 2^{2^d} + R$ with $0 \leq R < 2^k\ 2^{2^k}$ and k is $O(\log\log N)$. Thus, for a block of length 2^k the the number of occurrences in the last tail of R positions can have an error in the order of 2^k times 2^k. This already explains the term $O(\log N)^2$ in the discrepancy bound stated in Theorem 1 It is carefully counted in Levin's chain of estimates [12, Lemma 5], [12, Corollaries 1 and 2] and the end of the proof of [12, Theorem 2].

5.2. **Proof of Theorem 2.** It follows from Propositions 7, 13 and 14.

Acknowledgements

The authors are members of the Laboratoire International Associé INFINIS, CONICET/Universidad de Buenos Aires–CNRS/Université Paris Diderot and they are partially supported by the ECOS project PA17C04. The second author is partially funded by the DeLTA project (ANR-16-CE40-0007).

References

[1] N. Álvarez, V. Becher, P. A. Ferrari, and S. A. Yuhjtman. Perfect necklaces. *Advances of Applied Mathematics*, 80:48–61, 2016.

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

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

[4] N. G. de Bruijn. A combinatorial problem. *Koninklijke Nederlandse Akademie v. Wetenschappen*, 49:758–764, 1946. Indagationes Mathematicae 8 (1946) 461-467.

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

[6] H. Faure. Discrépance de suites associées à un système de numération (en dimension s). *Acta Arithmetica*, 41, 1982.

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

[8] 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.

[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 upper bounds of discrepancy of completely uniform distributed and normal sequences. *Abstracts American Mathematical Society*, 16:556–557, 1995. AMS-IMU joint meeting, Jerusalem, Israel, May 24–26, 1995.

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

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

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

[15] Edgardo Ugalde. An alternative construction of normal numbers. *Journal de Théorie des Nombres de Bordeaux*, 12:165–177, 2000.

Verónica Becher
Departamento de Computación, Facultad de Ciencias Exactas y Naturales & ICC
Universidad de Buenos Aires & CONICET, Argentina
vbecher@dc.uba.ar

Olivier Carton
Institut de Recherche en Informatique Fondamentale
Université Paris Diderot, France
Olivier.Carton@irif.fr