ACTA ARITHMETICA
158.4 (2013)

A generalization of NUT digital $(0,1)$-sequences and best possible lower bounds for star discrepancy

by

Henri Faure (Marseille) and Friedrich Pillichshammer (Linz)

1. Introduction. In this study, we are interested in irregularities of distribution of a class of one-dimensional sequences that generalize van der Corput sequences $X = (x_n)_{n\geq 1}$ in base b ($b \geq 2$ an integer), where

$$x_n = \frac{a_0(n)}{b} + \frac{a_1(n)}{b^2} + \frac{a_2(n)}{b^3} + \cdots$$

whenever $n-1$ has b-adic digit expansion $n-1 = a_0(n) + a_1(n)b + a_2(n)b^2 + \cdots$. The sequences considered in this paper are one-dimensional projections of special (t,s)-sequences, a broad family of s-dimensional sequences introduced by Niederreiter following former constructions due to Sobol' and Faure (see, for instance, [5, 24] and the references therein). Apart from such sequences being of interest in the theory of uniform distribution, (t,s)-sequences are of great importance for quasi-Monte-Carlo (QMC) methods in numerical analysis, most notably in numerical integration.

We study irregularities of distribution in terms of different notions of discrepancy, like for example the star discrepancy which can be defined as follows: for a sequence $X = (x_n)_{n\geq 1}$ in $[0,1]$ and for an integer $N \geq 1$ the star discrepancy is given by

$$D^*(N,X) = \sup_{0\leq\alpha\leq 1} |\#\{n \in \mathbb{N} : 1 \leq n \leq N \text{ and } x_n \in [0,\alpha)\} - N\alpha|.$$

A sequence X is uniformly distributed modulo one if and only if its normalized star discrepancy $D^*(N,X)/N$ tends to zero as N goes to infinity. Furthermore, the normalized star discrepancy can be used to bound the absolute integration error of a QMC algorithm applied to functions of bounded variation via the Koksma–Hlawka inequality. For more information we refer to [5, 7, 19]. More notions of discrepancy will be introduced in Section 2.

2010 *Mathematics Subject Classification*: 11K38, 11K31.
Key words and phrases: irregularity of distribution, discrepancy, diaphony, digital sequence, van der Corput sequence.

DOI: 10.4064/aa158-4-2

As announced in the title, our aim is to generalize digital $(0,1)$-sequences generated by non-singular upper triangular (NUT) matrices (see Section 3 for precise definitions). This will be done in a way that retains the properties of these sequences (as shown in [11]), but which also permits the use of arbitrary permutations instead of just multiplications (by the diagonal entries of the NUT matrix). Concerning QMC methods, this extension will enlarge the choices of "good" scramblings for the construction of efficient multi-dimensional point sets which can avoid correlations induced by linear scramblings in some situations (recall that in [15] and [22] lots of numerical experiments using Halton sequences and $(0,s)$-sequences have been successfully handled using such linear scramblings resulting from [11] through the selection criteria worked out in [12]). Further research in this direction is left for future work. For the moment, generalizing results from [11], we obtain exact formulas for different notions of discrepancy of generalized digital $(0,1)$-sequences (see Theorem 1). As an application, from the formula for star discrepancy we obtain best possible lower bounds for many subclasses of $(0,1)$-sequences. This way we extend results on shifted van der Corput sequences in base 2 from [6, 18, 20, 21].

The following sections are devoted to basic definitions (Section 2), to background information on $(0,1)$-sequences (Section 3) and to our generalization as announced above (Section 4). The best possible lower bounds on star discrepancy will be presented in Section 5.

2. Discrepancies. In uniform distribution theory, discrepancy is a quantitative measure for the irregularity of distribution modulo one of a sequence. The analysis of the discrepancy of a sequence represents an important field in number theory. Furthermore, it is well known that the discrepancy of a sequence is directly linked to the QMC-integration error for different classes of functions. See, for example, [1, 5, 19, 24] for more information in these two directions. In the following we recall the definition of the most important discrepancies. As in this paper we consider only one-dimensional sequences, we restrict ourselves to this case.

Let $X = (x_n)_{n\geq 1}$ be an infinite sequence in $[0,1]$, let $N \geq 1$ be an integer and let $[\alpha,\beta)$ be a subinterval of $[0,1]$. Then the *discrepancy function* or *error to ideal distribution* is the difference

$$E([\alpha,\beta);N;X) = A([\alpha,\beta);N;X) - N\lambda([\alpha,\beta)),$$

where $A([\alpha,\beta);N;X)$ is the number of indices n such that $1 \leq n \leq N$ and $x_n \in [\alpha,\beta)$ and where $\lambda([\alpha,\beta))$ is the length of $[\alpha,\beta)$.

The L_∞ *discrepancies* of X are defined by

$$\begin{aligned} D(N,X) &= \sup_{0\le\alpha<\beta\le 1} |E([\alpha,\beta);N;X)|,\\ D^*(N,X) &= \sup_{0\le\alpha\le 1} |E([0,\alpha);N;X)|,\\ D^+(N,X) &= \sup_{0\le\alpha\le 1} E([0,\alpha);N;X),\\ D^-(N,X) &= \sup_{0\le\alpha\le 1} (-E([0,\alpha);N;X)). \end{aligned}$$

Usually, D is called the *extreme discrepancy* and D^* the *star discrepancy* of X. The quantities D^+ and D^- are linked to them by

$$\begin{aligned} D(N,X) &= D^+(N,X) + D^-(N,X),\\ D^*(N,X) &= \max(D^+(N,X), D^-(N,X)). \end{aligned}$$

Note that $D^* \le D \le 2D^*$.

The L_2 *discrepancy* and the *diaphony* of X are defined by

$$\begin{aligned} T(N,X) &= \Big(\int_0^1 E^2\left([0,\alpha);N;X\right)\, d\alpha\Big)^{1/2},\\ F(N,X) &= \left(2\sum_{m=1}^{\infty}\frac{1}{m^2}\Big|\sum_{n=1}^{N}\exp(2\pi\mathtt{i}mx_n)\Big|^2\right)^{1/2}, \end{aligned}$$

respectively. They are linked together by the formula of Koksma

$$T^2(N,X) = \left(\sum_{n=1}^{N}\left(\frac{1}{2}-x_n\right)\right)^2 + \frac{1}{4\pi^2}F^2(N,X).$$

Note that $\sum_{n=1}^{N}(1/2-x_n) = \int_0^1 E([0,\alpha);N;X)\,d\alpha$ so that (see [4, Prop. 2.3]) $F^2(N,X) = 2\pi^2\int_0^1\int_0^1 E^2\left([\alpha,\beta);N;X\right)\, d\alpha\, d\beta$.

To end this section, recall that a sequence X is uniformly distributed modulo one if and only if its discrepancies (except D^+ and D^-) and diaphony both normalized by N go to zero as N tends to infinity.

3. Review of $(0,1)$-sequences. A typical example of a one-dimensional sequence with low discrepancy is the van der Corput sequence which is the prototype of (t,s)-sequences as introduced by Sobol', Faure and Niederreiter. In this section we provide a short review of existing concepts of $(0,1)$-sequences.

3.1. Generalized van der Corput sequences. This type of sequences has been introduced by Faure [9]. Let $b \ge 2$ be an integer. For integers n

and N with $n \geq 1$ and $1 \leq N \leq b^n$, write the b-adic expansion of $N-1$ as

$$N-1 = \sum_{r=0}^{n-1} a_r(N) b^r \tag{1}$$

and let $\Sigma = (\sigma_r)_{r\geq 0}$ be a sequence of permutations of $\{0,1,\ldots,b-1\}$.

Then the *generalized van der Corput sequence* S_b^Σ in base b associated with Σ is defined by

$$S_b^\Sigma(N) = \sum_{r=0}^{\infty} \frac{\sigma_r\big(a_r(N)\big)}{b^{r+1}} \tag{2}$$

for integers $N \geq 1$. If $(\sigma_r)_{r\geq 0} = (\sigma)_{r\geq 0}$ is constant, we simply write $S_b^\Sigma = S_b^\sigma$. The *original van der Corput sequence* S_b^{id} in base b is obtained with the identical permutation id.

3.2. (0, 1)-sequences in base b. The concept of (t,s)-sequences has been introduced by Niederreiter (see [5, 24]) to give a general framework for various constructions of s-dimensional low discrepancy sequences and to obtain further constructions. Smaller values of the so-called quality parameter $t \geq 0$ give smaller discrepancies. In order to provide new important constructions, Tezuka [31] and then Niederreiter and Xing [26], [27] (see also the more recent [25]) introduced a generalized definition which uses the so-called truncation: Let $x \in [0,1]$ with a prescribed b-adic expansion $x = \sum_{i=1}^{\infty} x_i b^{-i}$, with the possibility that $x_i = b-1$ for all but finitely many i. For every integer $m \geq 1$, define the *m-truncated expansion* of x by $[x]_{b,m} = \sum_{i=1}^{m} x_i b^{-i}$.

An *elementary interval in base b* is an interval of the form $[a/b^d, (a+1)/b^d)$ with integers a, d such that $d \geq 0$ and $0 \leq a < b^d$.

A sequence $(x_N)_{N\geq 1}$ (with prescribed b-adic expansions for each x_N) is a $(0,1)$-*sequence in base b (in the broad sense)* if for all integers $l, m \geq 0$, every elementary interval E with $\lambda(E) = b^{-m}$ contains exactly one element of the point set

$$\{[x_N]_{b,m} \,:\, lb^m + 1 \leq N \leq (l+1)b^m\}.$$

The original definition of $(0,1)$-sequences in base b due to Niederreiter is the same but with $[x_N]_{b,m}$ replaced by x_N. These sequences are nowadays known as $(0,1)$-sequences in base b *in the narrow sense* and the general construction is just named $(0,1)$-sequences in base b (see Niederreiter and Xing [27, Definition 2 and Remark 1]). Sometimes, we will add the term "in the broad sense" if we want to emphasize the difference.

3.3. Digital (0, 1)-sequences over $\mathbb{Z}_b$. For an integer $b \geq 2$ let $\mathbb{Z}_b = \mathbb{Z}/b\mathbb{Z}$ be the residue class ring modulo b equipped with addition and multiplication modulo b.

Instead of permutations as in Section 3.1, here we consider the action of infinite $\mathbb{N}\times\mathbb{N}$ matrices over $\mathbb{Z}_b$ on the digits of $N-1$. The general framework goes back to Niederreiter [24] (see also [5]), but a simpler formulation for the one-dimensional case in base 2 was given in [20, 29]. The following definition is an extension to arbitrary bases b.

Let $C=(c_k^r)_{r\ge0,k\ge0}$ be an infinite matrix with entries $c_k^r\in\mathbb{Z}_b$ such that for any integer $m\ge1$ every left upper $m\times m$ submatrix of C is non-singular. Then a *digital* $(0,1)$*-sequence* X_b^C in base b associated with C is an infinite sequence defined for all integers $N\ge1$ by

$$X_b^C(N)=\sum_{r=0}^{\infty}\frac{x_{N,r}}{b^{r+1}}\quad\text{where}\quad x_{N,r}=\sum_{k=0}^{\infty}c_r^k a_k(N)\pmod b, \tag{3}$$

with the $a_k(N)$ defined as in (1). Note that the second summation is finite and performed in $\mathbb{Z}_b$, but the first one can be infinite with the possibility that $x_{N,r}=b-1$ for all but finitely many r. Of course, we obtain the original van der Corput sequence S_b^{id} with the identity matrix I, i.e., we have $S_b^{\mathrm{id}}=X_b^I$.

Generalized van der Corput sequences as defined in (2) and digital $(0,1)$-sequences as defined in (3) are both $(0,1)$-sequences in base b in the broad sense; see [13, Proposition 3.1]. The truncation is required for sequences S_b^Σ in the case when $\sigma_r(0)=b-1$ for all sufficiently large r and for sequences X_b^C in the case when the matrix C provides digits $x_{N,r}=b-1$ for all sufficiently large r.

3.4. NUT digital $(0,1)$-sequences over $\mathbb{Z}_b$. An important special case of digital $(0,1)$-sequences is obtained when the associated matrix C is a non-singular upper triangular (NUT) matrix. In this case the first summation in (3) is finite as well. These sequences are now called *NUT digital* $(0,1)$*-sequences over* $\mathbb{Z}_b$ (in the narrow sense). In [11] the first author proved valuable formulas for the different notions of discrepancies of NUT digital $(0,1)$-sequences over $\mathbb{Z}_b$ in the case when b is a *prime number*.

To recall these formulas we first need to introduce some standard definitions used in the study of van der Corput sequences. Let $\mathfrak{S}_b$ be the set of all permutations of $\mathbb{Z}_b$. For any $\sigma\in\mathfrak{S}_b$ set

$$\mathcal{Z}_b^\sigma=(\sigma(0)/b,\sigma(1)/b,\dots,\sigma(b-1)/b).$$

For $h\in\{0,1,\dots,b-1\}$ and $x\in[(k-1)/b,k/b)$ where $k\in\{1,\dots,b\}$, define

$$\varphi_{b,h}^\sigma(x)=\begin{cases}A([0,h/b);k;\mathcal{Z}_b^\sigma)-hx & \text{if } 0\le h\le\sigma(k-1),\\ (b-h)x-A([h/b,1);k;\mathcal{Z}_b^\sigma) & \text{if } \sigma(k-1)<h<b.\end{cases}$$

Further, the functions $\varphi_{b,h}^\sigma$ are extended to the reals by periodicity. Based on $\varphi_{b,h}^\sigma$ we define further functions which then appear in the formulas for

different notions of discrepancy. Put

$$\psi_b^{\sigma,+} = \max_{0\le h<b} \varphi_{b,h}^{\sigma}, \quad \psi_b^{\sigma,-} = \max_{0\le h<b} (-\varphi_{b,h}^{\sigma}), \quad \psi_b^{\sigma} = \psi_b^{\sigma,+} + \psi_b^{\sigma,-},$$

$$\varphi_b^{\sigma} = \sum_{h=0}^{b-1} \varphi_{b,h}^{\sigma}, \qquad \phi_b^{\sigma} = \sum_{h=0}^{b-1} (\varphi_{b,h}^{\sigma})^2, \qquad \chi_b^{\sigma} = b\phi_b^{\sigma} - (\varphi_b^{\sigma})^2.$$

Note that

$$\psi_b^{\sigma} = \max_{0\le h<h'<b} |\varphi_{b,h}^{\sigma} - \varphi_{b,h'}^{\sigma}| \quad \text{and} \quad \chi_b^{\sigma} = \sum_{0\le h<h'<b} (\varphi_{b,h}^{\sigma} - \varphi_{b,h'}^{\sigma})^2. \tag{4}$$

Then, we need further definitions to deal with NUT digital $(0,1)$-sequences. The symbol $\uplus$ is used to denote the translation (or shift) of a given permutation $\sigma \in \mathfrak{S}_b$ by an element $t \in \mathbb{Z}_b$ in the following sense:

$$(\sigma \uplus t)(i) := \sigma(i) + t \pmod b \quad \text{for all } i \in \mathbb{Z}_b,$$

and for any integer $r \ge 0$ we introduce the quantity

$$\theta_r(N) := \sum_{k=r+1}^{\infty} c_r^k a_k(N) \pmod b,$$

where the $a_k(N)$ are the digits of $N-1$ as in (1). Note that $a_k(N) = 0$ for all $k \ge n$ if $1 \le N \le b^n$, thus $\theta_r(N) = 0$ for all $r \ge n-1$ in this case. This quantity determines the translated permutations that appear in the formulas for D^+, D^-, D^* and T. Finally, we define the permutation δ_r by $\delta_r(i) := c_r^r i \pmod b$ for $i \in \mathbb{Z}_b$.

Based on the definitions given above we can state formulas for the different notions of discrepancy of a NUT digital $(0,1)$-sequence (see [11, Theorems 1–4]): for any NUT digital $(0,1)$-sequence X_b^C over $\mathbb{Z}_b$ and for any integer $N \ge 1$, we have

$$D^+(N, X_b^C) = \sum_{j=1}^{\infty} \psi_b^{\delta_{j-1} \uplus \theta_{j-1}(N),+}\left(\frac{N}{b^j}\right),$$

$$D^-(N, X_b^C) = \sum_{j=1}^{\infty} \psi_b^{\delta_{j-1} \uplus \theta_{j-1}(N),-}\left(\frac{N}{b^j}\right),$$

$$D(N, X_b^C) = \sum_{j=1}^{\infty} \psi_b^{\delta_{j-1}}\left(\frac{N}{b^j}\right),$$

$$T^2(N, X_b^C) = \frac{1}{b} \sum_{j=1}^{\infty} \phi_b^{\delta_{j-1} \uplus \theta_{j-1}(N)}\left(\frac{N}{b^j}\right) + \frac{1}{b^2} \sum_{i \ne j} \varphi_b^{\delta_{i-1} \uplus \theta_{i-1}(N)}\left(\frac{N}{b^i}\right) \varphi_b^{\delta_{j-1} \uplus \theta_{j-1}(N)}\left(\frac{N}{b^j}\right),$$

$$\frac{1}{4\pi^2} F^2(N, X_b^C) = \frac{1}{b^2} \sum_{j=1}^{\infty} \chi_b^{\delta_{j-1}}\left(\frac{N}{b^j}\right).$$

4. Generalized NUT $(0,1)$-sequences over $\mathbb{Z}_b$. We now introduce a mixed construction which contains both generalized van der Corput sequences and NUT digital $(0,1)$-sequences over $\mathbb{Z}_b$. The idea is to put arbitrary permutations in place of the diagonal entries of the NUT matrix C defining a NUT digital $(0,1)$-sequence. Moreover, the construction is valid for *arbitrary* bases b.

DEFINITION 1. For any integer $b \geq 2$, let $\Sigma = (\sigma_r)_{r\geq 0} \in \mathfrak{S}_b^{\mathbb{N}}$ and let $C = (c_r^k)_{r\geq 0,\, k\geq r+1}$ be a strict upper triangular matrix with entries in $\mathbb{Z}_b$. Then, for all integers $N \geq 1$, the Nth element of the sequence $X_b^{\Sigma,C}$ is defined by

$$X_b^{\Sigma,C}(N) = \sum_{r=0}^{\infty} \frac{x_{N,r}}{b^{r+1}} \quad \text{where} \tag{5}$$

$$x_{N,r} = \sigma_r(a_r(N)) + \sum_{k=r+1}^{\infty} c_r^k a_k(N) \pmod b,$$

with the $a_k(N)$ defined as in (1). We call $X_b^{\Sigma,C}$ a *NUT* $(0,1)$*-sequence* over $\mathbb{Z}_b$.

If all entries of C are zero, then we have $X_b^{\Sigma,C} = S_b^{\Sigma}$, the generalized van der Corput sequences. If $\sigma_r = \delta_r$ for all $r \geq 0$ with δ_r as in Section 3.4, then we have $X_b^{\Sigma,C} = X_b^{C'}$, the NUT digital $(0,1)$-sequences with associated matrix $C' = (c_r^k)_{r\geq 0,\, k\geq r}$ obtained from C by putting *invertible* entries $c_r^r \in \mathbb{Z}_b$ on the diagonal. Every NUT $(0,1)$-sequence over $\mathbb{Z}_b$ is a $(0,1)$-sequence in the broad sense. The proof of this fact is the same as the proof of [13, Proposition 3.1] for generalized van der Corput sequences.

It is quite remarkable that [11, Theorems 1–4] for NUT digital $(0,1)$-sequences in prime base b are still valid for that generalization. Roughly speaking, the basic idea is to keep bijections of $\mathbb{Z}_b$ "on the diagonal"—the only place where we need to compute inverses; all other operations concerning entries above the diagonal are performed in the ring $\mathbb{Z}_b$.

THEOREM 1. *With the notations introduced in Section* 3.4, *for all integers* $b \geq 2$ *and* $N \geq 1$, *we have*

$$D^+(N, X_b^{\Sigma,C}) = \sum_{j=1}^{\infty} \psi_b^{\sigma_{j-1} \uplus \theta_{j-1}(N),+}\left(\frac{N}{b^j}\right), \tag{6}$$

$$D^-(N, X_b^{\Sigma,C}) = \sum_{j=1}^{\infty} \psi_b^{\sigma_{j-1} \uplus \theta_{j-1}(N),-}\left(\frac{N}{b^j}\right), \tag{7}$$

$$D(N, X_b^{\Sigma,C}) = \sum_{j=1}^{\infty} \psi_b^{\sigma_{j-1}}\left(\frac{N}{b^j}\right), \tag{8}$$

$$T^2(N, X_b^{\Sigma,C}) = \frac{1}{b}\sum_{j=1}^{\infty} \phi_b^{\sigma_{j-1}\uplus\theta_{j-1}(N)}\left(\frac{N}{b^j}\right) + \frac{1}{b^2}\sum_{i\neq j} \varphi_b^{\sigma_{i-1}\uplus\theta_{i-1}(N)}\left(\frac{N}{b^i}\right)\varphi_b^{\sigma_{j-1}\uplus\theta_{j-1}(N)}\left(\frac{N}{b^j}\right), \tag{9}$$

$$\frac{1}{4\pi^2}F^2(N, X_b^{\Sigma,C}) = \frac{1}{b^2}\sum_{j=1}^{\infty} \chi_b^{\sigma_{j-1}}\left(\frac{N}{b^j}\right). \tag{10}$$

The proof of Theorem 1, which is rather complex and needs a lot of prerequisites, follows closely the proofs of [11, Theorems 1–4]. However, several technical changes are required, taking into account the fact that with arbitrary permutations we can have $\sigma_r(0) \neq 0$ for some or for all $r \geq 0$, whereas in [11], $\delta_r(0) = c_r^r 0 = 0$ for all $r \geq 0$. For these reasons, instead of going into the details, we will only give a sketch of the proof where we point out the differences compared to [11].

The reader mainly interested in best possible lower bounds for the star discrepancy of $(0,1)$-sequences can skip the proof (Sections 4.1–4.3) and move directly to Section 5.

4.1. Three basic properties of $X_b^{\Sigma,C}$ sequences. We need more notations to state these properties. Let $X_n = (x_1, \ldots, x_{b^n})$ and $Y_n = (y_1, \ldots, y_{b^n})$ where $x_N := X_b^{\Sigma,C}(N)$ and $y_N := S_b^{\mathrm{id}}(N)$ for $1 \leq N \leq b^n$. Denote by $\overline{X}_n$ and $\overline{Y}_n$ the supports (i.e. the sets of elements) of X_n and Y_n ($\overline{Y}_n$ is the so-called set of n-bit numbers, with $y_1 = 0$). Since $x_1 = \sum_{r=0}^{\infty} \sigma_r(0) b^{-r-1}$, we only have $x_1 = 0$ if $\sigma_r(0) = 0$ for all $r \geq 0$, which is the case with NUT digital sequences X_b^C. But in general $\overline{X}_n \neq \overline{Y}_n$. This is an important difference between the sequences $X_b^{\Sigma,C}$ and X_b^C, which requires a careful adaptation of the proofs. Finally, for all non-negative integers l, m we define the segments $X_m^l := (x_{lb^m+1}, \ldots, x_{(l+1)b^m})$ of a sequence X. In particular we have $X_n = X_n^0$. These segments have already been used in Section 3.2 for the definition of $(0,1)$-sequences in base b, but with the truncated expansions of x_N. Here we consider the full expansions, which implies that the reals $x_N \in [0,1]$ are not necessarily n-bit numbers in general.

PROPERTY 1. *For any integer $n \geq 1$, the elements of X_n are the vertices (including x_1) of a regular polygon of b^n edges inscribed in $[0,1]$ identified with the unit torus. Moreover, let i, j be integers with $1 \leq i \leq b^{n-1}$ and $0 \leq j < b$, and let $x_i := x_{i,0}b^{-1} + \cdots + x_{i,n-2}b^{-n+1}$ be the b-adic expansion of x_i. Then*

$$x_{i+jb^{n-1}} = \sigma_{n-1}(j)b^{-n} + (x_{i,0} + c_0^{n-1}j)b^{-1} + \cdots + (x_{i,n-2} + c_{n-2}^{n-1}j)b^{-n+1} + \cdots$$

is the b-adic expansion of $x_{i+jb^{n-1}}$ (where of course the digits $x_{i,n-k} + c_{n-k}^{n-1}j$ are computed modulo b).

The proof of this property is the same as for [11, Property 5.1] but with the diagonal entries c_r^r of the NUT matrix replaced by the permutations σ_r.

The next two properties deal with the order of terms in segments X_m^l of X_n compared to the order of terms in the various $\mathcal{Z}_b^\sigma$ coming from Σ and C. The first one is concerned with $X_n = X_n^0$ and the next one with strict segments of X_n. These properties are fundamental tools which permit the derivation of the exact formulas stated in Theorem 1.

PROPERTY 2. *Let $n \geq 1$, let $u \in \overline{Y}_{n-1}$ with b-adic expansion $u = \sum_{r=0}^{n-2} u_r b^{-r-1}$ and set $v = u + b^{-n+1}$. Then the interval $[u, v)$ contains exactly b terms of X_n, which are given in increasing order by*

$$u \leq x_{i_0+j_0 b^{n-1}} < x_{i_1+j_1 b^{n-1}} < \cdots < x_{i_{b-1}+j_{b-1} b^{n-1}} < v,$$

where, for $0 \leq \mu \leq b-1$, $j_\mu = \sigma_{n-1}^{-1}(\mu)$ and i_μ is a well defined integer with $1 \leq i_\mu \leq b^{n-1}$ depending on u (its exact form can be obtained from the proof). Therefore, the order of the terms of X_n in $[u, v)$ is independent of $u \in \overline{Y}_{n-1}$, and it is the same as the order of the terms of $\mathcal{Z}_b^{\sigma_{n-1}}$ in $[0, 1)$, given by

$$0 = \sigma_{n-1}(j_0) < \sigma_{n-1}(j_1) < \cdots < \sigma_{n-1}(j_{b-1}) = b-1.$$

In contrast to the study of generalized van der Corput sequences S_b^Σ in [9, Prop. 3.1.3] and [4, Prop. 3.2], the terms of X_n in $[u, v)$ are not determined by the indices $i + jb^{n-1}$ of Property 1 for fixed i and $0 \leq j < b$. The situation is more complicated and the index i is not fixed. Moreover, in general $j_0 = \sigma_{n-1}^{-1}(0) \neq 0$, which implies that $u < x_{i_0+j_0 b^{n-1}}$ in this case. Apart from that, the proof follows the lines of the proof of [11, Property 5.2], with the solution of an upper triangular system of n linear equations in n variables (with parameter μ), except on the diagonal, where invertible entries are replaced with arbitrary permutations.

For short, from now on, we set $\rho_r := \sigma_r \uplus \theta_r(N)$ for the permutations involved in Theorem 1.

PROPERTY 3. *Let n and s be integers with $2 \leq s \leq n$. Let $u \in \overline{Y}_{n-s}$ with b-adic expansion $u = \sum_{r=0}^{n-s-1} u_r b^{-r-1}$ (put $u = 0$ if $s = n$) and set $v = u + b^{-n+s}$. Let $A_{n-s+1} := \sum_{r=n-s+1}^{n-1} z_r b^r$ with arbitrary given digits $z_{n-1}, \ldots, z_{n-s+1}$ and let $S_{n-s+1} := X_{n-s+1}^{A_{n-s+1} b^{-n+s-1}}$ be the corresponding segment of X_n. Then the interval $[u, v)$ contains exactly b terms of S_{n-s+1}, which are given in increasing order by*

$$u \leq x_{i_0+j_0 b^{n-s}+A_{n-s+1}} < x_{i_1+j_1 b^{n-s}+A_{n-s+1}} < \cdots < x_{i_{b-1}+j_{b-1} b^{n-s}+A_{n-s+1}} < v$$

where, for $0 \leq \mu \leq b-1$, $j_\mu = \rho_{n-s}^{-1}(\mu)$ and i_μ is an integer with $1 \leq i_\mu \leq b^{n-s}$ depending on u. Therefore the order of the terms of S_{n-s+1} in $[u, v)$ is independent of $u \in \overline{Y}_{n-s}$, and is the same as the order of the terms of

$\mathcal{Z}_b^{\rho_{n-s}}$ *in* $[0,1)$ *given by*

$$0 = \rho_{n-s}(j_0) < \rho_{n-s}(j_1) < \cdots < \rho_{n-s}(j_{b-1}) = b-1.$$

For the proof of Property 2 we had to solve a system of n equations in n unknowns and parameter μ whereas now we have a system of $n-s+1$ equations in $n-s+1$ unknowns and parameters $(z_{n-1},\dots,z_{n-s+1})$ and μ. First we obtain $\mu = \sigma(z_{n-s}) + c_{n-s}^{n-s+1} z_{n-s+1} + \cdots + c_{n-s}^{n-1} z_{n-1}$, which is equivalent to $z_{n-s} = \sigma_{n-s}^{-1}(\mu - c_{n-s}^{n-s+1} z_{n-s+1} + \cdots + c_{n-s}^{n-1} z_{n-1}) = j_\mu = \rho_{n-s}^{-1}(\mu)$. The remainder of the proof is then straightforward and is the same as in the proof of [11, Property 5.3].

4.2. Three lemmas for the discrepancy function of $X_b^{\Sigma,C}$. The following lemma is just a discretization of the discrepancy function. For short, from now on, we write $E(\alpha,N,X) := E([0,\alpha);N;X)$.

LEMMA 1. *Let* $\alpha \in [0,1]$ *and let* n,N *be integers with* $1 \le N \le b^n$. *Furthermore, let* $u,v \in \overline{Y}_n$ *be such that* $u \le \alpha < v$ *and* $v = u + b^{-n}$ *and let* x *be the unique element in* $\overline{X}_n$ *such that* $u \le x < v$. *Then, with* $y(\alpha) := u$ *if* $\alpha \le x$ *and* $y(\alpha) := v$ *if* $\alpha > x$, *we have*

$$E(\alpha,N,X_b^{\Sigma,C}) = E(y(\alpha),N,X_b^{\Sigma,C}) + (y(\alpha)-\alpha)N.$$

This is a classical discretization property resulting from the definition of $y(\alpha)$ which implies that $A(\alpha,N,X_b^{\Sigma,C}) = A(y(\alpha),N,X_b^{\Sigma,C})$. The formulation is a bit more complex than that of [11, Lemma 6.1] and requires further attention in the proof of (9).

From Lemma 1 it follows that it suffices to know the values of the discrepancy function $E(\alpha,N,X_b^{\Sigma,C})$ for α of the form $\alpha = \lambda/b^n$ with integers $1 \le \lambda < b^n$. Exactly these values are given by the following lemma which will be the key property in the proof of Theorem 1.

LEMMA 2. *Let* n, N *and* λ *be integers with* $1 \le N \le b^n$ *and* $1 \le \lambda < b^n$ *and let* $\lambda = \lambda_1 b^{n-1} + \cdots + \lambda_{n-1} b + \lambda_n$ *be the* b*-adic expansion of* λ. *Then*

$$E\left(\frac{\lambda}{b^n},N,X_b^{\Sigma,C}\right) = \sum_{j=1}^{n} \varphi_{b,\varepsilon_j}^{\sigma_{j-1}\uplus\theta_{j-1}(N)}\left(\frac{N}{b^j}\right).$$

The functions $\varepsilon_j = \varepsilon_j(\lambda,n,N)$ *are defined inductively by* $\varepsilon_n = \eta_n = \lambda_n$ *and, for* $1 \le j < n$,

$$\eta_j = \lambda_j + \frac{\eta_{j+1}}{b} + \frac{1}{b}(\varphi_{b,\varepsilon_{j+1}}^{\sigma_j\uplus\theta_j(N)})'\left(\frac{N}{b^{j+1}}\right), \qquad \varepsilon_j = \begin{cases} \eta_j & \text{if } 0 \le \eta_j < b, \\ 0 & \text{if } \eta_j = b. \end{cases}$$

The proof is a descending recursion for the b-adic resolution of the argument $y = \lambda/b^n$ from n to 1. At each step, the b-adic resolution of y is decreased by 1. The differences between the discrepancy functions in a reduction step are kept under control by means of the functions $\varphi_{b,h}^{\rho}$. For the

initial reduction step, Property 2 is required with the permutation σ_{n-1}. For the further steps Property 3 is used with the permutation ρ_{n-s}. Although the proof is intricate, it repeats almost exactly the proof of [11, Lemma 6.2]. The changes are only marginal and concern the permutations δ_r on the diagonal of the NUT matrix which now have to be replaced by permutations σ_r. We omit the details and refer the reader to [11].

The following lemma shows how the functions ε_j can be computed explicitly. This lemma is required for the proof of (9) dealing with the L_2 discrepancy.

LEMMA 3. *With the notations of Lemma* 1*, let* $N \geq 1$ *be an integer with* b*-adic expansion* $N = \sum_{r=0}^{n-1} N_r b^r$*, and for* $0 \leq j \leq n-1$ *set*

$$\Lambda_j = \sum_{r=j+1}^{n} \lambda_r b^{n-r} \quad \text{and} \quad \nu_j = \sum_{r=j}^{n-1} \sigma_r(N_r) b^{n-r-1}.$$

Then for $1 \leq j \leq n-1$ *we have*

$$\eta_j = \begin{cases} \lambda_j & \text{if } 0 \leq \Lambda_j \leq \nu_j, \\ \lambda_j + 1 & \text{if } \nu_j \leq \Lambda_j < b^{n-j}, \end{cases}$$

and

$$\varepsilon_j = \begin{cases} 0 & \text{if } 0 \leq \Lambda_{j-1} \leq \nu_j, \\ p & \text{if } \nu_j + (p-1)b^{n-j} < \Lambda_{j-1} \leq \nu_j + pb^{n-j} \text{ (for } 1 \leq p < b), \\ 0 & \text{if } \nu_j + (b-1)b^{n-j} < \Lambda_{j-1} < b^{n-j+1}. \end{cases}$$

Lemma 3 was first proved in [4] for the study of the L_2 discrepancy of generalized van der Corput sequences in variable bases $B = (b_j)_{j \geq 0}$, with $b_0 = 1$ and $b_j \geq 2$ for all $j \geq 1$. In [11] the proof for fixed bases ($b_j = b$ for all $j \geq 1$) has been outlined. We refer to these papers and do not repeat the proof.

4.3. The proof of Theorem 1. We split the proof into proofs of formulas (6)–(10).

Proof of (6) *and* (7) *for* D^+ *and* D^-. This proof follows exactly the lines of the proof of [11, Theorem 1]. We give the guidelines for (6). Formula (7) can be obtained in the same way.

Let $N \geq 1$ be a fixed integer and n an arbitrary integer satisfying $N \leq b^n$. From Lemma 1, we get (for a detailed proof, see [9, Lemme 3.3.1])

$$\lim_{n \to \infty} \sup_{y \in \overline{Y}_n} E(y, N, X_b^{\Sigma,C}) = D^+(N, X_b^{\Sigma,C}).$$

Then, since $\psi_b^{\sigma,+} = \max_{0 \leq h < b} \varphi_{b,h}^{\sigma}$, for all $y = \lambda/b^n \in \overline{Y}_n$, from Lemma 2 we get

$$E(y, N, X_b^{\Sigma,C}) \leq \sum_{j=1}^{n} \psi_b^{\rho_{j-1},+}\left(\frac{N}{b^j}\right), \quad \text{where} \quad \rho_{j-1} = \sigma_{j-1} \uplus \theta_{j-1}(N).$$

Now, using the algorithm for the construction of the ε_j's from the λ_j's (at the end of Lemma 2) in reverse direction, it is easy to construct a $\lambda_* \in \overline{Y}_n$ for which the above upper bound is achieved by $E(\lambda_* b^{-n}, N, X_b^{\Sigma,C})$. Finally, letting $n \to \infty$ gives formula (6). ∎

REMARK 1. In the special case where C is the null matrix, formulas (6) and (7) provide a new and simpler proof of [9, Théorème 1] for S_b^Σ.

Proof of (9) *for* L_2 *discrepancy.* In contrast to the proof of [11, Theorem 3] for the L_2 discrepancy of NUT digital $(0,1)$-sequences, the elements $X_b^{\Sigma,C}(N)$ are not n-bit numbers anymore for $1 \le N \le b^n$. Hence, at the beginning, we have to follow the more involved proof of [4, Theorem 4.1] for the L_2 discrepancy of sequences S_B^Σ in variable base B. We only give the necessary hints (in fixed base b).

The goal is to compute $T^2(N, X_b^{\Sigma,C}) := \int_0^1 E^2(\alpha, N, X_b^{\Sigma,C})\, d\alpha$. Applying Lemma 1 with $u = (\lambda-1)b^{-n}$ for $1 \le \lambda \le b^n$, we obtain a unique $x'_\lambda \in \overline{X}_n$ such that

$$E(\alpha, N, X_b^{\Sigma,C}) =: E(\alpha, N) = \begin{cases} E((\lambda-1)/b^n, N) + ((\lambda-1)/b^n - \alpha)N & \text{if } (\lambda-1)/b^n \le \alpha \le x'_\lambda, \\ E(\lambda/b^n, N) + (\lambda/b^n - \alpha)N & \text{if } x'_\lambda < \alpha < \lambda/b^n. \end{cases}$$

We then split the integral over the intervals $[(\lambda-1)/b^n, x'_\lambda]$ and $[x'_\lambda, \lambda/b^n]$ for $1 \le \lambda \le b^n$ and obtain after some computations

$$\begin{aligned} T^2(N, X_b^{\Sigma,C}) &= \frac{1}{b^n}\sum_{\lambda=1}^{b^n} E^2\left(\frac{\lambda}{b^n}, N\right) + \frac{N}{b^n}\sum_{\lambda=1}^{b^n} E\left(\frac{\lambda}{b^n}, N\right)\left(\frac{2\lambda}{b^n} - x'_\lambda - x'_{\lambda-1}\right) \\ &\quad + \frac{N^2}{3b^n}\sum_{\lambda=1}^{b^n-1}\left(\left(\frac{\lambda}{b^n} - x'_\lambda\right)^2 + \left(\frac{\lambda}{b^n} - x'_{\lambda+1}\right)\left(\frac{\lambda}{b^n} - x'_\lambda\right) + \left(\frac{\lambda}{b^n} - x'_{\lambda+1}\right)^2\right) \\ &\quad + N^2({x'_1}^3 + (1 - x'_{b^n})^3). \end{aligned}$$

But, due to Property 2, $(\lambda/b^n - x'_\lambda)$ is independent of λ and the formula reduces to

$$\begin{aligned} T^2(N, X_b^{\Sigma,C}) &= \frac{1}{b^n}\sum_{\lambda=1}^{b^n} E^2\left(\frac{\lambda}{b^n}, N\right) + \frac{N}{b^n}\left(\frac{1}{b^n} - 2x'_1\right)\sum_{\lambda=1}^{b^n} E\left(\frac{\lambda}{b^n}, N\right) \\ &\quad + \frac{1}{N^2}\left({x'_1}^2 - \frac{x'_1}{b^n} + \frac{1}{3b^{2n}}\right). \end{aligned}$$

From now on, the proof follows [11, Section 6.5]: Using Lemma 2, we obtain an expression involving the functions $\varphi_{b,\varepsilon_j}^{\rho_{j-1}}$ for the two sums above. Then, according to Lemma 3, we can divide the set of λ_j's into classes where the

$\varepsilon_j = p$ are constant, hence recovering the functions $\varphi_b^{\rho_{j-1}}$ and $\phi_b^{\rho_{j-1}}$ in (9). Finally, the two sums read as follows:

$$\sum_{\lambda=1}^{b^n} E\left(\frac{\lambda}{b^n}, N\right) = b^{n-1} \sum_{j=1}^{n} \varphi_b^{\rho_{j-1}}\left(\frac{N}{b^j}\right),$$

$$\sum_{\lambda=1}^{b^n} E^2\left(\frac{\lambda}{b^n}, N\right) = b^{n-1} \sum_{j=1}^{n} \phi_b^{\rho_{j-1}}\left(\frac{N}{b^j}\right) + 2b^{n-2} \sum_{1\le i<j\le n} \varphi_b^{\rho_{i-1}}\left(\frac{N}{b^i}\right)\varphi_b^{\rho_{j-1}}\left(\frac{N}{b^j}\right).$$

Inserting back into $T^2(N, X_b^{\Sigma,C})$ and letting $n \to \infty$ gives the result (note that $x_1' \to 0$ as $n \to \infty$). ∎

Proof of (8) *and* (10) *for the discrepancy* D *and the diaphony* F. The formulas with permutations $\rho_r := \sigma_r \uplus \theta_r(N)$,

$$D(N, X_b^{\Sigma,C}) = \sum_{j=1}^{\infty} \psi_b^{\rho_{j-1}}\left(\frac{N}{b^j}\right) \quad \text{and} \quad \frac{1}{4\pi^2} F^2(N, X_b^{\Sigma,C}) = \frac{1}{b^2} \sum_{j=1}^{\infty} \chi_b^{\rho_{j-1}}\left(\frac{N}{b^j}\right),$$

directly follow from the relations $D = D^+ + D^-$ and $\psi_b^\sigma = \psi_b^{\sigma,+} + \psi_b^{\sigma,-}$ for D and from the Koksma formula for F, respectively. Now formulas (8) and (10) follow from a general property of shifted permutations:

PROPERTY 4. *For any* $\sigma \in \mathfrak{S}_b$ *and* $t \in \mathbb{Z}_b$, $\psi_b^{\sigma \uplus t} = \psi_b^\sigma$ *and* $\chi_b^{\sigma \uplus t} = \chi_b^\sigma$.

The proof of this property is based on the formulas stated in (4); see [11, Proposition 6.6] or [4, Theorem 4.4] for details. ∎

5. Application: Best possible lower bounds for D^*. In this section, we give an application of Theorem 1 and show best possible lower bounds on the star discrepancy of NUT $(0,1)$-sequences. This study is motivated by a best possible lower bound on the star discrepancy of digitally shifted van der Corput sequences in base 2 shown in [18] and the question whether this bound remains true also for digitally shifted NUT digital sequences in base 2 (see Corollary 4 for an answer).

5.1. Overview of the problem. For an infinite sequence X in $[0,1)$, set

$$s(X) := \limsup_{N\to\infty} \frac{D(N,X)}{\log N} \quad \text{and} \quad s^*(X) := \limsup_{N\to\infty} \frac{D^*(N,X)}{\log N}.$$

A famous theorem of Schmidt [30], further improved by Béjian [3], states that for any sequence X in $[0,1)$ we have $s(X) \ge 0.12$ and hence $s^*(X) \ge 0.06$.

On the other hand, it has been known for a long time that this lower bound is best possible: for the van der Corput sequence S_2^{id} in base 2, Haber [16] has shown that $s(S_2^{\mathrm{id}}) = 1/(3\log 2) = 0.4808\ldots$. Since then, finding sequences with the lowest possible discrepancy has interested several people trying to reduce the gap between upper and lower bounds. Two families of sequences received particular attention in the last decades: $(n\alpha)$ sequences and generalized van der Corput sequences. Among many results, we recall only those giving the best sequences with regard to star discrepancy in these two families:

• Concerning the star discrepancy of $(n\alpha)$ sequences, Dupain and Sós [8] proved that

$$\inf_{\alpha} s^*((n\alpha)) = s^*((n\sqrt{2})) = \frac{1}{4\log(\sqrt{2}+1)} = 0.2836\ldots. \tag{11}$$

• Concerning the star discrepancy of generalized van der Corput sequences, things cannot be stated so definitely. It is possible to give best possible results among subfamilies of sequences S_b^{Σ} but not on the whole family, which is too large since there are too many possible choices of sequences of permutations Σ. Until now, all improvements are based on [9, Théorème 3] (see also [14] for a review), which reads as follows:

Let $\tau \in \mathfrak{S}_b$ be the permutation defined by $\tau(k) = b-k-1$ for all $k \in \mathbb{Z}_b$ and let $\mathcal{A}$ be the subset of $\mathbb{N}_0$ defined by $\mathcal{A} = \bigcup_{H=1}^{\infty} \mathcal{A}_H$ with $\mathcal{A}_H = \{H(H-1), \ldots, H^2-1\}$. For any permutation $\sigma \in \mathfrak{S}_b$, let $\overline{\sigma} := \tau \circ \sigma$ and let

$$\Sigma_{\mathcal{A}}^{\sigma} = (\sigma_r)_{r\ge 0} := (\sigma, \overline{\sigma}, \sigma, \sigma, \overline{\sigma}, \overline{\sigma}, \sigma, \sigma, \sigma, \overline{\sigma}, \overline{\sigma}, \overline{\sigma}, \ldots)$$

be the sequence of permutations defined by $\sigma_r = \sigma$ if $r \in \mathcal{A}$ and $\sigma_r = \overline{\sigma}$ if $r \notin \mathcal{A}$. Then

$$s^*(S_b^{\Sigma_{\mathcal{A}}^{\sigma}}) = \frac{\alpha_b^{\sigma,+} + \alpha_b^{\sigma,-}}{2\log b}, \tag{12}$$

where

$$\alpha_b^{\sigma,+} = \inf_{n\ge 1} \frac{1}{n} \sup_{x\in[0,1]} \sum_{j=1}^{n} \psi_b^{\sigma,+}\left(\frac{x}{b^j}\right),$$

$$\alpha_b^{\sigma,-} = \inf_{n\ge 1} \frac{1}{n} \sup_{x\in[0,1]} \sum_{j=1}^{n} \psi_b^{\sigma,-}\left(\frac{x}{b^j}\right).$$

For reasonably small b, the constants $\alpha_b^{\sigma,+}$ and $\alpha_b^{\sigma,-}$ are not difficult to compute, and for the identical permutation, in which case $\psi_b^{\mathrm{id},-} = 0$, it is

even possible to find them explicitly. We have (see [2, 18] for $b = 2$ and [9, Théorème 6] for arbitrary b)

$$s(S_b^{\Sigma_{\mathcal{A}}^{\mathrm{id}}}) = s^*(S_b^{\Sigma_{\mathcal{A}}^{\mathrm{id}}}) = \frac{\alpha_b^{I,+}}{2\log b} = \begin{cases} \dfrac{b-1}{8\log b} & \text{if } b \text{ is odd,} \\ \dfrac{b^2}{8(b+1)\log b} & \text{if } b \text{ is even.} \end{cases}$$

The smallest star discrepancy currently known was recently obtained by Ostromoukhov [28, Theorem 5] in base 60: there exists a permutation $\sigma_0 \in \mathfrak{S}_{60}$ such that

$$s^*(S_{60}^{\Sigma_{\mathcal{A}}^{\sigma_0}}) = \frac{32209}{35400\log 60} = 0.2222\ldots,$$

improving a preceding result in [9, Théorème 5] with a permutation $\sigma_1 \in \mathfrak{S}_{12}$ giving $s^*(S_{12}^{\Sigma_{\mathcal{A}}^{\sigma_1}}) = 0.2235\ldots$. It is interesting to note that $\psi_{12}^{\sigma_1,-} \neq 0$ whereas $\psi_{60}^{\sigma_0,-} = 0$. This last property is quite remarkable in view of the multitude of permutations involved in the computational search for $(60, \sigma_0)$ among all pairs (b, σ).

5.2. Getting best possible lower bounds with S_b^{Σ} sequences. In order to highlight the property that permits the finding of best possible lower bounds in subfamilies of $X_b^{\Sigma,C}$ sequences, we recall the part played by the permutation τ in [9, Théorème 3]. Let $\mathcal{S}$ be a subset of $\mathbb{N}_0$ and let $\sigma \in \mathfrak{S}_b$. Define the sequence $\Sigma_{\mathcal{S}}^{\sigma} = (\sigma_r)_{r\geq 0}$ by $\sigma_r = \sigma$ if $r \in \mathcal{S}$ and $\sigma_r = \overline{\sigma} = \tau \circ \sigma$ if $r \notin \mathcal{S}$. Then, by [9, Lemme 4.4.1] or [14, Section 5],

$$D^+(N, S_b^{\Sigma_{\mathcal{S}}^{\sigma}}) = \sum_{j=1,\, j\in\mathcal{S}}^{\infty} \psi_b^{\sigma,+}\left(\frac{N}{b^j}\right) + \sum_{j=1,\, j\notin\mathcal{S}}^{\infty} \psi_b^{\sigma,-}\left(\frac{N}{b^j}\right),$$

$$D^-(N, S_b^{\Sigma_{\mathcal{S}}^{\sigma}}) = \sum_{j=1,\, j\in\mathcal{S}}^{\infty} \psi_b^{\sigma,-}\left(\frac{N}{b^j}\right) + \sum_{j=1,\, j\notin\mathcal{S}}^{\infty} \psi_b^{\sigma,+}\left(\frac{N}{b^j}\right).$$

The permutation τ swaps the functions $\psi_b^{\sigma,+}$ and $\psi_b^{\sigma,-}$ and hence, to minimize $D^* = \max(D^+, D^-)$, one has to find a set $\mathcal{S}$ for which the sums with $\psi_b^{\sigma,+}$ and $\psi_b^{\sigma,-}$ asymptotically divide into two equal parts. This is achieved, among others, by the set $\mathcal{A} = \{0, 2, 3, 6, 7, 8, 12, 13, 14, 15, \ldots\}$. Moreover, for any $\mathcal{S} \subseteq \mathbb{N}_0$, we have

$$\begin{aligned} D(N, S_b^{\Sigma_{\mathcal{S}}^{\sigma}}) &= D^+(N, S_b^{\Sigma_{\mathcal{S}}^{\sigma}}) + D^-(N, S_b^{\Sigma_{\mathcal{S}}^{\sigma}}) \\ &= \sum_{j=1}^{\infty} \left(\psi_b^{\sigma,+}\left(\frac{N}{b^j}\right) + \psi_b^{\sigma,-}\left(\frac{N}{b^j}\right) \right) = D(N, S_b^{\sigma}), \end{aligned}$$

since $\psi_b^{\sigma,+} + \psi_b^{\sigma,-} = \psi_b^\sigma$. Hence we obtain

$$D^*(N, S_b^{\Sigma_{\mathcal{S}}^\sigma}) \ge \frac{1}{2} D(N, S_b^{\Sigma_{\mathcal{S}}^\sigma}) = \frac{1}{2} D(N, S_b^\sigma),$$

which implies

$$s^*(S_b^{\Sigma_{\mathcal{S}}^\sigma}) \ge \frac{1}{2} s(S_b^\sigma) = \frac{\alpha_b^\sigma}{2 \log b}, \tag{13}$$

because by [9, Théorème 2] we have

$$s(S_b^\sigma) = \frac{\alpha_b^\sigma}{\log b} \quad \text{with} \quad \alpha_b^\sigma = \inf_{n \ge 1} \frac{1}{n} \sup_{x \in [0,1]} \sum_{j=1}^{n} \psi_b^\sigma \left(\frac{x}{b^j} \right).$$

However, in general we have $\alpha_b^\sigma \le \alpha_b^{\sigma,+} + \alpha_b^{\sigma,-}$. Hence we cannot infer any relation between the general lower bound on $s^*(S_b^{\Sigma_{\mathcal{S}}^\sigma})$ from (13) and the upper bound on $s^*(S_b^{\Sigma_{\mathcal{A}}^\sigma})$ from (12). Only if for the permutation σ we have either $\psi_b^{\sigma,+} = 0$ or $\psi_b^{\sigma,-} = 0$, in which case we get $\alpha_b^\sigma = \alpha_b^{\sigma,+} + \alpha_b^{\sigma,-}$, do we infer that $\alpha_b^\sigma/(2 \log b)$ is the best possible lower bound for the star discrepancy of sequences S_b^Σ with $\Sigma \in \{\sigma, \overline{\sigma}\}^{\mathbb{N}}$. In other words,

$$\inf_{\Sigma \in \{\sigma, \tau \circ \sigma\}^{\mathbb{N}}} s^*(S_b^\Sigma) = \frac{\alpha_b^\sigma}{2 \log b}$$

for any $\sigma \in \mathfrak{S}_b$ such that $D^*(S_b^\sigma) = D(S_b^\sigma)$. (Recall that for any $\Sigma = (\sigma_r)_{r \ge 0}$ we have $D^*(S_b^\Sigma) = D(S_b^\Sigma)$ if and only if $\psi_b^{\sigma_r,+} = 0$ for all $r \ge 0$ or $\psi_b^{\sigma_r,-} = 0$ for all $r \ge 0$; see [9, Corollaire 2, p. 160]).

5.3. Best possible lower bounds for $X_b^{\Sigma,C}$ sequences. The process applied to S_b^Σ sequences in Section 5.2 can also be applied to $X_b^{\Sigma,C}$ sequences. This leads to best possible lower bounds on the star discrepancy for larger subfamilies of low discrepancy sequences.

THEOREM 2. *For any integer $b \ge 2$, let $\sigma \in \mathfrak{S}_b$ and let C be a strict upper triangular matrix with entries in $\mathbb{Z}_b$. Then, for any subset $\mathcal{S}$ of $\mathbb{N}_0$, we have* (*see Section* 5.2 *for the meaning of* $\Sigma_{\mathcal{S}}^\sigma$)

$$D^*(N, X_b^{\Sigma_{\mathcal{S}}^\sigma, C}) \ge \frac{1}{2} D(N, S_b^\sigma) \quad \textit{and hence} \quad s^*(X_b^{\Sigma_{\mathcal{S}}^\sigma, C}) \ge \frac{\alpha_b^\sigma}{2 \log b}.$$

Proof. From (8) in Theorem 1, we obtain

$$D(N, X_b^{\Sigma_{\mathcal{S}}^\sigma, C}) = \sum_{j=1}^{\infty} \psi_b^{\sigma_{j-1}} \left(\frac{N}{b^j} \right) = \sum_{j=1}^{\infty} \psi_b^\sigma \left(\frac{N}{b^j} \right) = D(N, S_b^\sigma),$$

since $\sigma_{j-1} \in \Sigma_{\mathcal{S}}^\sigma$ so that $\sigma_{j-1} = \sigma$ or $\tau \circ \sigma$ and hence $\psi_b^{\sigma_{j-1}} = \psi_b^\sigma$ for all $j \ge 1$. Now the result follows in the same way as in Section 5.2. ∎

COROLLARY 1. *Let* $\mathcal{C}_{\mathrm{SUT}}$ *be the set of all strict upper triangular matrices and let* $\sigma \in \mathfrak{S}_b$ *be such that* $D^*(S_b^\sigma) = D(S_b^\sigma)$*. Then*

$$\inf_{\substack{\Sigma \in \{\sigma, \tau\circ\sigma\}^{\mathbb{N}} \\ C \in \mathcal{C}_{\mathrm{SUT}}}} s^*(X_b^{\Sigma,C}) = \frac{\alpha_b^\sigma}{2\log b}.$$

Proof. Theorem 2 implies that $\alpha_b^\sigma/(2\log b)$ is a lower bound, and on the other hand, with the null matrix $C = 0$ and $\Sigma_{\mathcal{A}}^\sigma$, we have $X_b^{\Sigma_{\mathcal{A}}^\sigma,0} = S_b^{\Sigma_{\mathcal{A}}^\sigma}$ so that

$$s^*(X_b^{\Sigma_{\mathcal{A}}^\sigma,0}) = s^*(S_b^{\Sigma_{\mathcal{A}}^\sigma}) = \frac{\alpha_b^\sigma}{2\log b}$$

by (12) since in the present case we have $\alpha_b^\sigma = \alpha_b^{\sigma,+} + \alpha_b^{\sigma,-}$. ∎

REMARK 2. Besides the identity id, it is not difficult to find permutations satisfying the condition of Corollary 1. This can be done, for example, by using intricate permutations (see, for instance, [10, Section 2.3] for the definition of intrication of two permutations). Moreover, a systematic computer search performed by F. Pausinger (IST Austria) has given respectively 26, 58, 340, and 1496 such permutations in bases 6, 7, 8, and 9. Further, we already observed in Section 5.1 that the best sequence (with respect to star discrepancy) currently known, namely $S_{60}^{\Sigma_{\mathcal{A}}^{\sigma_0}}$, satisfies this condition. Hence in base $b = 60$ we have

$$\inf_{\substack{\Sigma \in \{\sigma_0, \tau\circ\sigma_0\}^{\mathbb{N}} \\ C \in \mathcal{C}_{\mathrm{SUT}}}} s^*(X_{60}^{\Sigma,C}) = 0.2222\ldots.$$

This value is much better than the corresponding value for the best $(n\alpha)$ sequence given in (11).

The case of identity in Corollary 1 is of special interest because α_b^{id} is explicitly known for any integer $b \geq 2$ (see Section 5.1).

COROLLARY 2. *With the notations of Corollary* 1*, we obtain*

$$\inf_{b\geq 2} \inf_{\substack{\Sigma \in \{\mathrm{id}, \tau\}^{\mathbb{N}} \\ C \in \mathcal{C}_{\mathrm{SUT}}}} s^*(X_b^{\Sigma,C}) = \frac{1}{4\log 3} = 0.2275\ldots.$$

This result can be seen as the analog for van der Corput sequences and NUT $(0,1)$-sequences of (11) for $(n\alpha)$ sequences. Compared to the best $(n\alpha)$ sequences here we still obtain a much smaller value for s^*.

Another interesting result, stemming from the case where $\sigma = \mathrm{id}$, concerns linearly digit scrambled NUT digital $(0,1)$-sequences. A *linear digit scrambling* is a permutation $\pi \in \mathfrak{S}_b$ of the form $\pi(k) = \gamma k + l \pmod b$ for all $k \in \mathbb{Z}_b$, with $\gamma \neq 0, l \in \mathbb{Z}_b$ (see [23] where the term is introduced together with many other scramblings). A *linearly digit scrambled NUT digital* $(0,1)$*-sequence*, denoted $Z_b^{\Pi,C}$, is defined as follows: Let $\mathcal{C}_{\mathrm{NUT}}^1$ be the

set of NUT matrices C such that all the diagonal entries $c_r^r = 1$ and let $\Pi = (\pi_r)_{r\ge 0} \in \mathfrak{S}_b^{\mathbb{N}}$ be a sequence of linear digit scramblings. Then, for any $N \ge 1$, set (see (1) for the meaning of $a_k(N)$)

$$Z_b^{\Pi,C}(N) = \sum_{r=0}^{\infty} \frac{\pi_r(x_{N,r})}{b^{r+1}} \quad \text{with} \quad x_{N,r} = \sum_{k=r}^{\infty} c_r^k a_k(N) \pmod b.$$

Corollary 3. *Let $Z_b^{\Pi,C}$ be a linearly digit scrambled NUT digital $(0,1)$-sequence associated with $C \in \mathcal{C}_{\mathrm{NUT}}^1$ and $\Pi = (\pi_r)_{r\ge 0} \in \{\mathrm{id}, \tau\}^{\mathbb{N}}$. Then*

$$\inf_{b\ge 2} \inf_{\substack{\Pi\in\{\mathrm{id},\tau\}^{\mathbb{N}} \\ C\in\mathcal{C}_{\mathrm{NUT}}^1}} s^*(Z_b^{\Pi,C}) = \frac{1}{4\log 3} = 0.2275\ldots.$$

Proof. The permutation τ is a linear digit scrambling since $\tau(k) = (b-1)k + b - 1 \pmod b$, so that

$$\begin{aligned}\tau(x_{N,r}) &= \tau\Big(\sum_{k=r}^{\infty} c_r^k a_k(N)\Big) = (b-1)\sum_{k=r}^{\infty} c_r^k a_k(N) + (b-1) \pmod b \\ &= (b-1)a_r(N) + (b-1) + \sum_{k=r+1}^{\infty} (b-1)c_r^k a_k(N) \pmod b.\end{aligned}$$

Hence $Z_b^{\Pi,C} = X_b^{\Pi,C'}$ with $C' = ((b-1)c_r^k)_{r\ge 0, k\ge r+1} \in \mathcal{C}_{\mathrm{SUT}}$. The result follows. ∎

Remark 3. It seems that Corollary 3 only concerns a very special sequence of linear digit scramblings. But in fact it is not difficult to see that id and τ are the only linear digit scramblings π satisfying $D^*(S_b^\pi) = D(S_b^\pi)$.

Finally, we give some special attention to the case $b = 2$. Following a lot of papers dealing with base $b = 2$ (see, for example, [18, 20, 21, 29]) we began the present study with the following question: "Is it true that the constant $1/(6\log 2)$ is best possible for any *digitally shifted NUT digital sequence in base* 2, as is the case for any digitally shifted van der Corput sequence according to [18, Corollary 4]?" Taking into account that, in base 2, τ is the non-zero shift and the diagonal entries of C are all equal to 1 we can answer this question in the affirmative as a special case of Corollary 3.

Corollary 4. *We have*

$$\inf_{\substack{\Delta\in\mathbb{Z}_2^{\mathbb{N}} \\ C\in\mathcal{C}_{\mathrm{NUT}}}} s^*(Z_2^{\Delta,C}) = \frac{1}{6\log 2} = 0.2404\ldots.$$

Acknowledgements. This study has been finalized during an invited stay of the first author at the University of Linz (Austria). We thank Florian

Pausinger for his computations (see Remark 2) and the anonymous referee for the careful reading of the manuscript and for many valuable remarks.

The second author is supported by the Austrian Science Foundation (FWF), Project S9609, that is part of the Austrian National Research Network "Analytic Combinatorics and Probabilistic Number Theory".

References

[1] J. Beck and W. W. L. Chen, *Irregularities of Distribution*, Cambridge Univ. Press, Cambridge, 1987.

[2] R. Béjian, *Sur certaines suites présentant une faible discrépance à l'origine*, C. R. Acad. Sci. Paris Sér. A 286 (1978), 135–138.

[3] R. Béjian, *Minoration de la discrépance d'une suite quelconque sur* $\boldsymbol{T}$, Acta Arith. 41 (1982), 185–202.

[4] H. Chaix and H. Faure, *Discrépance et diaphonie en dimension un*, Acta Arith. 63 (1993), 103–141.

[5] J. Dick and F. Pillichshammer, *Digital Nets and Sequences. Discrepancy Theory and Quasi-Monte Carlo Integration*, Cambridge Univ. Press, Cambridge, 2010.

[6] M. Drmota, G. Larcher and F. Pillichshammer, *Precise distribution properties of the van der Corput sequence and related sequences*, Manuscripta Math. 118 (2005), 11–41.

[7] M. Drmota and R. F. Tichy, *Sequences, Discrepancies and Applications*, Lecture Notes in Math. 1651, Springer, Berlin, 1997.

[8] Y. Dupain and V. T. Sós, *On the discrepancy of* $(n\alpha)$ *sequences*, in: Topics in Classical Number Theory (Budapest, 1981), Vol. I, Colloq. Math. Soc. János Bolyai 34, North-Holland, Amsterdam, 1984, 355–387.

[9] H. Faure, *Discrépances de suites associées à un système de numération* (*en dimension un*), Bull. Soc. Math. France 109 (1981), 143–182.

[10] H. Faure, *Good permutations for extreme discrepancy*, J. Number Theory 42 (1992), 47–56.

[11] H. Faure, *Discrepancy and diaphony of digital* $(0,1)$*-sequences in prime base*, Acta Arith. 117 (2005), 125–148.

[12] H. Faure, *Selection criteria for* (*random*) *generation of digital* $(0,s)$*-sequences*, in: Monte Carlo and Quasi-Monte Carlo Methods 2004, H. Niederreiter and D. Talay (eds.), Springer, Berlin, 2006, 113–126.

[13] H. Faure, *Van der Corput sequences towards* $(0,1)$*-sequences in base* b, J. Théor. Nombres Bordeaux 19 (2007), 125–140.

[14] H. Faure, *Improvements on low discrepancy one-dimensional sequences and two-dimensional point sets*, in: Monte-Carlo and Quasi-Monte Carlo Methods 2006, A. Keller et al. (eds.), Springer, New York, 2008, 327–341.

[15] H. Faure and C. Lemieux, *Generalized Halton sequences in 2008: A comparative study*, ACM Trans. Model. Comput. Simul. 19 (2009), No. 4, Article 15.

[16] S. Haber, *On a sequence of points of interest for numerical quadrature*, J. Res. Nat. Bur. Standards Sect. B 70 (1966), 127–136.

[17] P. Kritzer, *A new upper bound on the star discrepancy of* $(0,1)$*-sequences*, Integers 5 (2005), No. 3, A11.

[18] P. Kritzer, G. Larcher and F. Pillichshammer, *A thorough analysis of the discrepancy of shifted Hammersley and van der Corput point sets*, Ann. Mat. Pura Appl. 186 (2007), 229–250.

[19] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley, New York, 1974; reprint, Dover, Mineola, NY, 2006.

[20] G. Larcher and F. Pillichshammer, *Walsh series analysis of the L_2-discrepancy of symmetrisized points sets*, Monatsh. Math. 132 (2001), 1–18.

[21] G. Larcher and F. Pillichshammer, *Sums of distances to the nearest integer and the discrepancy of digital nets*, Acta Arith. 106 (2003), 379–408.

[22] C. Lemieux and H. Faure, *New perspectives on $(0, s)$-sequences*, in: Monte-Carlo and Quasi-Monte Carlo Methods 2008, P. L'Ecuyer and A. B. Owen (eds.), Springer, New York, 2009, 113–130.

[23] J. Matoušek, *On the L_2-discrepancy for anchored boxes*, J. Complexity 14 (1998), 527–556.

[24] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, CBMS-NSF Reg. Conf. Ser. Appl. Math. 63, SIAM, Philadelphia, 1992.

[25] H. Niederreiter and F. Özbudak, *Low-discrepancy sequences using duality and global function fields*, Acta Arith. 130 (2007), 79–97.

[26] H. Niederreiter and C. P. Xing, *Low-discrepancy sequences and global function fields with many rational places*, Finite Fields Appl. 2 (1996), 241–273.

[27] H. Niederreiter and C. P. Xing, *Quasirandom points and global functions fields*, in: Finite Fields and Applications, S. Cohen and H. Niederreiter (eds.), London Math. Soc. Lecture Note Ser. 233, Cambridge Univ. Press, Cambridge, 1996, 269–296.

[28] V. Ostromoukhov, *Recent progress in improvement of extreme discrepancy and star discrepancy of one-dimensional sequences*, in: Monte-Carlo and Quasi-Monte Carlo Methods 2008, P. L'Ecuyer and A. B. Owen (eds.), Springer, New York, 2009, 561–572.

[29] F. Pillichshammer, *On the discrepancy of $(0, 1)$-sequences*, J. Number Theory 104 (2004), 301–314.

[30] W. M. Schmidt, *Irregularities of distribution VII*, Acta Arith. 21 (1972), 45–50.

[31] S. Tezuka, *Polynomial arithmetic analogue of Halton sequences*, ACM Trans. Model. Comput. Simul. 3 (1993), 99–107.

Henri Faure
Institut de Mathématiques de Luminy (CNRS)
Université d'Aix-Marseille
163 avenue de Luminy, case 907
13288 Marseille Cedex 09, France
E-mail: faure@iml.univ-mrs.fr

Friedrich Pillichshammer
Institut für Finanzmathematik
Universität Linz
Altenbergerstraße 69
A-4040 Linz, Austria
E-mail: friedrich.pillichshammer@jku.at

Received on 23.1.2012
and in revised form on 21.1.2013 (6950)