DE GRUYTER OPEN

uniform distribution theory

DOI: 10.1515/udt-2018–0005
Unif. Distrib. Theory **13** (2018), no.1, 87–107

AN EXTENSION OF THE DIGITAL METHOD BASED ON b-ADIC INTEGERS

Roswitha Hofer — Ísabel Pirsic

ABSTRACT. We introduce a hybridization of digital sequences with uniformly distributed sequences in the domain of b-adic integers, $\mathbb{Z}_b, b \in \mathbb{N} \setminus \{1\}$, by using such sequences as input for generating matrices. The generating matrices are then naturally required to have finite row-lengths. We exhibit some relations of the 'classical' digital method to our extended version, and also give several examples of new constructions with their respective quality assessments in terms of $t, \mathbf{T}$ and discrepancy.

Communicated by Friedrich Pillichshammer

1. Introduction

Constructing sequences with good equidistribution properties is an important problem in number theory and has applications to quasi-Monte Carlo methods in numerical analysis (see, e.g., [2, 24]). In this context, the star discrepancy appears as an important measure of uniform distribution. For a given dimension $s \geq 1$, let J be a subinterval of $[0,1]^s$ and let $\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}$ be N points in $[0,1]^s$ (we speak also of a *point set* $\mathcal{P}$ of N points in $[0,1]^s$). We define the counting function A for the interval J by $A(J;\mathcal{P}) := \#\{0 \leq n < N : \boldsymbol{x}_n \in J\}$. Then the *star discrepancy* of the point set $\mathcal{P}$ consisting of the points $\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}$ is defined by

$$D_N^*(\mathcal{P}) = D_N^*(\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}) = \sup_J \left| \frac{A(J;\mathcal{P})}{N} - \mathrm{vol}(J) \right|,$$

where the supremum is extended over all subintervals J of $[0,1]^s$ with one vertex at the origin.

2010 Mathematics Subject Classification: 11J71, 11K16, 11K38, 11F85.
Keywords: quasi-Monte Carlo methods, construction, digital method, digit expansion, q-adic integers .

For a sequence $\mathcal{S}$ of points $\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots$ in $[0,1]^s$, the star discrepancy of the first N terms of $\mathcal{S}$ is defined as $D_N^*(\mathcal{S}) = D_N^*(\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1})$. The sequence $\mathcal{S}$ is called *uniformly distributed* if and only if $D_N^*(\mathcal{S}) \to 0$ as $N \to \infty$.

We say that $\mathcal{S}$ is a *low-discrepancy sequence* if

$$N D_N^*(\mathcal{S}) = O\big((\log N)^s\big) \qquad \text{for all } N \geq 2, \tag{1}$$

where the implied constant does not depend on N. It is conjectured that $O\big(N^{-1}(\log N)^s\big)$ is the least possible order of magnitude in N that can be obtained for the star discrepancy of a sequence of points in $[0,1]^s$.

Probably the most widespread technique for constructing low-discrepancy sequences is the *digital method* which was introduced by Niederreiter [23] and later slightly generalized in [26].

Algorithm 1. Choose a dimension $s \in \mathbb{N}$, a finite commutative ring R with identity and of order b, and set $Z_b = \{0, 1, \ldots, b-1\}$. Choose

(i) bijections $\psi_r : Z_b \to R$ for all integers $r \geq 0$, satisfying $\psi_r(0) = 0$ for all sufficiently large r;

(ii) elements $c_{j,r}^{(i)} \in R$ for $1 \leq i \leq s$, $j \geq 1$, $r \geq 0$;

(iii) bijections $\lambda_{i,j} : R \to Z_b$ for $1 \leq i \leq s$, $j \geq 1$.

The ith component $\boldsymbol{x}_n^{(i)}$ of the nth point $\boldsymbol{x}_n$ of the sequence $(\boldsymbol{x}_n)_{n\geq 0}$ is defined using the base b representation of $n = \sum_{r=0}^{\infty} a_r b^r$ with $a_r \in Z_b$ and $a_r = 0$ for all sufficiently large r as follows.

$$\boldsymbol{x}_n^{(i)} := \sum_{j=1}^{\infty} \lambda_{i,j} \left(\sum_{r=0}^{\infty} c_{j,r}^{(i)} \psi_r(a_r) \right) \Big/ b^j. \tag{2}$$

Note that the inner sum in (2) is a finite sum because of the choice that $\psi_r(0) = 0$ for all sufficiently large r and the fact that $a_r = 0$ for all sufficiently large r.

The presentation of the digital method often uses the concept of infinite *generating matrices*, $C^{(i)} := \big(c_{j,r}^{(i)}\big)_{j\geq 1, r\geq 0} \in R^{\mathbb{N}\times\mathbb{N}_0}$ for $i \in \{1, \ldots, s\}$ with the construction given as follows. Set

$$C^{(i)} \cdot \begin{pmatrix} \psi_0(a_0) \\ \psi_1(a_1) \\ \vdots \end{pmatrix} =: \begin{pmatrix} y_{n,1}^{(i)} \\ y_{n,2}^{(i)} \\ \vdots \end{pmatrix}.$$

Then,

$$\boldsymbol{x}_n^{(i)} = \sum_{j=1}^{\infty} \lambda_{i,j} \left(y_{n,j}^{(i)} \right) b^{-j}.$$

Obviously, the challenge is to find appropriate elements $c_{j,r}^{(i)} \in R$ such that the generated sequence $(\boldsymbol{x}_n)_{n\geq 0}$ is a low-discrepancy sequence.

Most of the actual constructions choose the ring R to be a finite field $\mathbb{F}_q$ with prime-power cardinality q. This has the advantage that basic linear algebra is available and the distribution of the generated sequence amongst elementary intervals is related to the rank-structure of the generating matrices.

An elementary interval in base b is an interval $I \subset [0,1]^s$ of the form

$$I = \prod_{i=1}^{s} \left[\frac{a_i}{b^{d_i}}, \frac{a_i+1}{b^{d_i}} \right)$$

with nonnegative integers $d_i, 0 \leq a_i < b^{d_i}$ for $i = 1, \ldots, s$.

The distribution amongst elementary intervals is relevant when determining the quality-parameter function $\mathbf{T}$ or the quality parameter t of the generated sequence when it is considered as a $(\mathbf{T}, s)$-sequence in base b in the sense of Larcher and Niederreiter [18] or a (t, s)-sequence in base b in the sense of Niederreiter [23]. Those concepts later have been modified by including truncation in [25, 27, 28] in order to meet certain requirements in special constructions. Throughout the paper $[x]_{b,m} := \sum_{j=1}^{m} x_j b^{-j}$ denotes the m-digit truncation of the real $x \in [0,1]$ in base b with a specific given base b representation $x = \sum_{j=1}^{\infty} x_j b^{-j}$, where the case that all but finitely many $x_j = b-1$ is explicitly admissible as well. For a vector the base b m-digit truncation is applied by coordinates.

Definition 1. Let b, t, m be integers satisfying $b \geq 2$ and $0 \leq t \leq m$. A (t, m, s)-*net in base* b is a point set of b^m points in $[0,1)^s$ such that every elementary interval $I \subseteq [0,1)^s$ in base b with volume b^{t-m} contains exactly b^t points of the point set.

Let $\mathbf{T} : \mathbb{N}_0 \to \mathbb{N}_0$ satisfying $\mathbf{T}(m) \leq m$ for all $m \in \mathbb{N}_0$. A sequence $\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots$ of points in $[0,1]^s$ is called a $(\mathbf{T}, s)$-*sequence in base* b if for all integers $k \geq 0$ and m satisfying $\mathbf{T}(m) < m$ the points $[\boldsymbol{x}_n]_{b,m}$ with $kb^m \leq n < (k+1)b^m$ form a $(\mathbf{T}(m), m, s)$-net in base b. As a special case, such a sequence is called a (t, s)-*sequence in base* b with $t \in \mathbb{N}_0$ if it is a $(\mathbf{T}, s)$-sequence in base b with $\mathbf{T}(m) \leq t$ for all $m \geq 0$.

A $(\mathbf{T}, s)$-sequence in base b is uniformly distributed if $\lim_{m\to\infty} \big(m - \mathbf{T}(m)\big) = \infty$. In particular, every (t, s)-sequence is uniformly distributed. Furthermore, if $\left(\frac{1}{r}\sum_{m=1}^{r} b^{\mathbf{T}(m)}\right)_{r\in\mathbb{N}}$ is bounded, then the $(\mathbf{T}, s)$-sequence in base b is a low-discrepancy sequence. Consequently, every (t, s)-sequence is a low-discrepancy sequence.

It is well-known that the digital method in Algorithm 1 applied to a finite field with cardinality q constructs a digital $(\mathbf{T}, s)$-sequence over $\mathbb{F}_q$ if and only if the following condition holds.

Condition 1. For every integer m satisfying $m > \mathbf{T}(m)$ and all nonnegative integers $d_1, \ldots, d_s \geq 0$ with $1 \leq d_1 + \cdots + d_s \leq m - \mathbf{T}(m)$, the $(d_1 + \cdots + d_s) \times m$ matrix over $\mathbb{F}_q$ formed by the row vectors

$$\left(c_{j,0}^{(i)}, c_{j,1}^{(i)}, \ldots, c_{j,m-1}^{(i)}\right) \in \mathbb{F}_q^m \quad \text{with} \quad 1 \leq j \leq d_i \quad \text{and} \quad 1 \leq i \leq s,$$

has rank $d_1 + \cdots + d_s$.

Analogously, Algorithm 1 produces a (t, s)-sequence if Condition 1 holds with $\mathbf{T}(m) = t$ for $m \geq t$ and $\mathbf{T}(m) = m$ else. Note that Algorithm 1 applied to a finite field with cardinality q generates a uniformly distributed sequence if and only if the following condition holds.

Condition 2. For every choice of $d_1, \ldots, d_s \geq 0$ (not all zero) the rows

$$\boldsymbol{c}_j^{(i)} = \left(c_{j,r}^{(i)}\right)_{r \geq 0}, \quad 1 \leq j \leq d_i, \quad 1 \leq i \leq s$$

are linearly independent over $\mathbb{F}_q$.

For more details on $(\mathbf{T}, s)$-sequences and their digital versions we refer the interested reader to [2, 24].

For reasons related to the uniform distribution of mixed-base digital sequences so-called finite-row generating matrices, i.e., matrices having in each row only finitely many nonzero entries, have been the subject of investigation. We refer to [6, 7, 9, 10, 12, 13, 14] for examples and constructions of finite-row generating matrices and more about their motivation. Note that the finite-row property of the matrices, i.e., for every $i = 1, \ldots, s$ and $j \geq 1$, $c_{j,r}^{(i)} = 0$ for all sufficiently large r, ensures the finiteness of the inner sum

$$\sum_{r=0}^{\infty} c_{j,r}^{(i)} \psi_r(a_r) \quad \text{in equation (2).}$$

Hence, when using finite-row generating matrices in the digital method, any sequence of bijections $(\psi_r)_{r \geq 0}$ can be used and the index sequence for the construction can in accordance be chosen freely as any sequence of b-adic integers, i.e., $\mathbb{Z}_b$, instead of just the nonnegative integers. Importantly, note that b is *not* required to be prime.

This yields the following alternative algorithm.

Algorithm 2. Choose a dimension $s \in \mathbb{N}$, a finite commutative ring R with identity and of order b, and set $Z_b = \{0, 1, \ldots, b-1\}$. Choose

(i) bijections $\psi_r : Z_b \to R$ for all integers $r \geq 0$;

(ii) elements $c_{j,r}^{(i)} \in R$ for $1 \leq i \leq s$, $j \geq 1$, $r \geq 0$, satisfying $c_{j,r}^{(i)} = 0$ for all sufficiently large r for fixed i, j;

(iii) bijections $\lambda_{i,j} : R \to Z_b$ for $1 \leq i \leq s$, $j \geq 1$.

(iv) a sequence $(s_n)_{n\geq 0}$ in $\mathbb{Z}_b$.

The ith component $\boldsymbol{x}_n^{(i)}$ of the nth point $\boldsymbol{x}_n$ of the sequence $(\boldsymbol{x}_n)$ is defined using the b-adic representation of $s_n = \sum_{r=0}^{\infty} a_r b^r$ with $a_r \in Z_b$ as follows.

$$\boldsymbol{x}_n^{(i)} = \sum_{j=1}^{\infty} \lambda_{i,j} \left(\sum_{r=0}^{\infty} c_{j,r}^{(i)} \psi_r(a_r) \right) / b^j. \tag{3}$$

Of course, one could generalize Algorithm 1 to subsequences indexed by $(s_n)_{n\geq 0} \in \mathbb{N}_0^{\mathbb{N}_0}$, whose elements have then all finite b-adic representations. Such subsequences were studied already, e.g., in [5, 8, 9, 11, 15]. The advantage of our Algorithm 2 is that this sequence $(s_n)_{n\geq 0}$ can be chosen over the b-adic integers $\mathbb{Z}_b$. E.g., we can consider the sequence $(-n-1)_{n\geq 0}$ or $(n/(b-1))_{n\geq 0}$, whose elements do not have finite b-adic representations. So for example for one-dimensional sequences constructed with the identity matrix, we can achieve sequence points with infinite digits, going beyond a simple digital or b-adic shift (as, e.g., considered in [4]). This also transports to higher dimensions. Hence Algorithm 2 is a considerable generalization of Algorithm 1.

The first objective is to have a criterion for uniform distribution of the so constructed sequences. This objective will be addressed in Section 3 of this paper. Of theoretical interest is the fact that Algorithm 2 transports uniform distribution in the b-adic integers to uniform distribution in the unit cube $[0,1]^s$ by a linear transformation.

Having uniform distribution the next natural question will be for estimates of the discrepancy of such sequences. Section 4 considers the discrepancy and quality parameter function $\mathbf{T}$ for sequences generated by Algorithm 2 using some specific $(s_n)_{n\geq 0}$ over $\mathbb{Z}_b$. This way we obtain low-discrepancy sequences, whose performance we will investigate and discuss numerically in Section 5.

The subsequent Section 2 recalls definitions pertaining to b-adic numbers and introduces some auxiliary results, that will be used in Section 3 and 4.

2. Relevant background on b-adic numbers

An introduction in and construction of b-adic integers and numbers for arbitrary integers $b \geq 2$ can, e.g., be found in [19]. Uniform distribution in the b-adic integers was introduced by Meijer [20], whose definitions we will employ and first briefly recall here. We use the name b-adic rather than g-adic, i.e., the letter b, to signify a not necessarily prime digit base, as is customary in the literature on uniform distribution modulo 1.

2.1. b-adic numbers and integers

(Detailed proofs for the claims in this section can be found in [20].)

Analogously to the case of p-adic numbers, b-adic numbers can be introduced as completion of $\mathbb{Q}$, only in this case not by a valuation (using the definition of Meijer, in the sense of an 'absolute value'), but the following pseudo-valuation.

Definition 2. Let $b \geq 2$ be a positive integer and $a \in \mathbb{Q}$ a rational. The prime decompositions of b, a, shall be given as

$$b = p_1^{\beta_1} \dots p_r^{\beta_r},\ a = \pm p_1^{\alpha_1} \dots p_s^{\alpha_s}, \quad \alpha_i \in \mathbb{Z}; \quad r, s, \beta_i \in \mathbb{N}.$$

Then the b-adic pseudo-valuation is defined by

$$|a|_b := \max_{i, p_i | b} b^{-\alpha_i/\beta_i}, \quad |0|_b := 0.$$

The 'pseudo' part signifies that the multiplicative identity demanded for a valuation only holds up to inequality, i.e.,

$$|mn|_b \leq |m|_b |n|_b.$$

Nevertheless, $d(x, y) := |x - y|_b$ is a (non-archimedean) metric, so the following definition is valid.

Definition 3. Let $b \geq 2$ be a positive integer. The ring obtained by completion of $\mathbb{Q}$ with respect to the b-adic pseudo-valuation shall be called the ring $\mathbb{Q}_b$ of b--adic numbers, and accordingly we define the subset

$$\mathbb{Z}_b := \left\{ a : a \in \mathbb{Q}_b, |a|_b \leq 1 \right\}$$

of b-adic integers.

We remark the following observations:

(1) Clearly, $\mathbb{Q} \subset \mathbb{Q}_b$, $\mathbb{Z} \subset \mathbb{Z}_b$, and $\mathbb{Z}_b$ is, indeed, a subring of $\mathbb{Q}_b$.

(2) $1/b < |a|_b \leq 1$ for $a \in \mathbb{N}, 1 \leq a < b$, where for composite b, values less than 1 can indeed occur, e.g.,

$$|6|_{24} = |18|_{24} = 1/\sqrt[3]{24},\ |12|_{24} = 1/\sqrt[3]{24^2}.$$

(3) For b prime, the definitions coincide with the usual notions. For composite b, we have the decomposition

$$\mathbb{Q}_b \cong \mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_r},$$

using the notation of Definition 2.

(4) As in the p-adic case, each $a \in \mathbb{Q}_b$ has a unique representation

$$a = \sum_{i=k_0}^{\infty} a_i b^i,$$

$$k_0 \in \mathbb{Z}, \quad a_i \in \{0, \ldots, b-1\}, \quad a_{k_0} \neq 0, \quad \text{and we have} \quad |a|_b = b^{-k_0}|a_{k_0}|_b.$$

For b-adic integers, $k_0 \geq 0$, i.e., we get a representation as a formal power series in b. Furthermore, for all $a \in \mathbb{N}_0$ the digit expansion in base b and the b-adic representation coincide.

(5) The number (in $\mathbb{Q}$) obtained by truncation of the unique representation of a number $a \in \mathbb{Q}_b$ at index $k \in \mathbb{Z}$ is defined by $\tau_k(a) := \sum_{i=k_0}^{k-1} a_i b^i$. A b-adic integer a is a unit if and only if $\gcd\big(\tau_1(a), b\big) = 1$. Moreover, if a is a unit, then $|a|_b = |a^{-1}|_b = 1$ (see [20, Lemma 4]).

2.2. Uniform distribution in $\mathbb{Z}_b$

First we recall the definition of uniform distribution in the rational integers $\mathbb{Z}$.

Definition 4. Let $\omega = (x_n)_{n\geq 0} \in \mathbb{N}_0^{\mathbb{N}_0}$ be a sequence of nonnegative integers, and $m \in \mathbb{N}$, $m > 1$. If for any a, $0 \leq a < m$ we have

$$\lim_{N\to\infty} \frac{\#\{n : x_n \equiv a \bmod m,\, n < N\}}{N} = \frac{1}{m},$$

ω is called uniformly distributed (u.d.) modulo m.

If ω is u.d. modulo m for any $m > 1$, it is called uniformly distributed in $\mathbb{Z}$.

The b-adic case models this very closely. However, here we require the 'local uniformity' only at powers of b.

Definition 5. Let $\omega = (x_n)_{n\geq 0} \in \mathbb{Z}_b^{\mathbb{N}_0}$ be a sequence of b-adic integers, and $k \in \mathbb{N}_0$. If for any a, $0 \leq a < b^k$ we have

$$\lim_{N\to\infty} \frac{\#\{n : |x_n - a|_b \leq b^{-k},\, n < N\}}{N} = \frac{1}{b^k},$$

ω is called k-uniformly distributed in $\mathbb{Z}_b$.

If ω is k-uniformly distributed for any $k \geq 1$, it is called uniformly distributed in $\mathbb{Z}_b$.

For reference we state the precise relation between the two notions as a lemma (cf. Corollary 1 in [21]). It is easily seen by the first observing that

$$\tau_k(x) \equiv a \bmod b^k \iff |x-a|_b \le b^{-k} \quad \text{for } x \in \mathbb{Z}_b,\ a \in \mathbb{N}_0,\ a < b^k,\ k \in \mathbb{N}_0.$$

Lemma 1. *A sequence $\omega = (x_n)_{n\ge 0} \in \mathbb{Z}_b^{\mathbb{N}_0}$ is u.d. in $\mathbb{Z}_b$ if and only if the sequences $\big(\tau_k(x_n)\big)_{n\ge 0} \in \mathbb{N}_0^{\mathbb{N}_0}$ are u.d. modulo b^k for every $k \ge 1$.*

Examples of uniformly distributed sequences in $\mathbb{Z}$ are the following as included in [20] and [17, Chapter 5]. By the previous definitions and lemma they can also be regarded as u.d. in $\mathbb{Z}_b$ for any $b \ge 2$.

(1) $(\lfloor \alpha n \rfloor)_{n\ge 0}$ for irrational $\alpha \in \mathbb{R} \setminus \mathbb{Q}$.

(2) $(\lfloor f(n) \rfloor)_{n\ge 0}$ for $f \in \mathbb{R}[x]$, where at least one coefficient that is not the constant is irrational.

(3) $(\lfloor \alpha n^\sigma \rfloor)_{n\ge 0}$ for $\alpha \in \mathbb{R}, \sigma \in \mathbb{R}^+ \setminus \mathbb{N}$.

From [20, Theorem 2] we know that $(n)_{n\ge 0}$ is u.d. in $\mathbb{Z}_b$. An example of how to obtain new u.d. sequences from other u.d. sequences is also given by [20, Theorem 3].

Lemma 2. *Let $a, c \in \mathbb{Z}_b$ and $(x_n)_{n\ge 0}$ be a sequence u.d. in $\mathbb{Z}_b$. Then the sequence $(ax_n + c)_{n\ge 0}$ is also u.d. in $\mathbb{Z}_b$ if and only if a is a unit.*

Consequently, $(an + c)_{n\ge 0}$ is u.d. in $\mathbb{Z}_b$, if a is a unit.

Example 1. Let a, c, d be b-adic integers such that $|a|_b < 1$ and c is a unit. Then the sequence $(an^2 + cn + d)_{n\ge 0}$ is uniformly distributed in $\mathbb{Z}_b$. (See [20, Theorem 5]). Furthermore, the sequence $(n^2)_{n\ge 0}$ is not uniformly distributed in $\mathbb{Z}_b$, which can be seen by quadratic residues modulo b^k.

2.3. The b-adic representation of b-adic integers

Obviously, the b-adic representation of a nonnegative integer corresponds to its base b digit expansion. This is not true for the negative integers, as is shown, e.g., by the b-adic representation of $-1 = \sum_{i=0}^{\infty}(b-1)b^i$. We recall the general situation and add some further details:

Lemma 3. *Let n be a positive (rational or b-adic) integer.*

– *The b-adic representation of $-n$ is related to the b-adic representation (or expansion) of $n = \sum_{i=r}^{\infty} a_i b^i$; $r \in \mathbb{N}_0$, $a_r \ne 0$ via*

$$-n = (b - a_r)b^r + \sum_{i=r+1}^{\infty} (b - 1 - a_i)b^i$$

(where $r = \min\{r' \in \mathbb{N}_0 : a_{r'} \ne 0\}$, i.e., $|n|_b = |a_r|_b b^{-r}$).

– *Let $k, l \in \mathbb{N}_0$ and $M = \{-n : kb^l < n \leq (k+1)b^l\}$. The b-adic integers in M share the same digits in their b-adic representations from index l on and run through all possible values in their first l digits.*
More precisely, if we denote the b-adic representation of a b-adic integer z by $z = \sum_{i=0}^{\infty} \overline{a}_i b^i$. Then $(\overline{a}_l, \overline{a}_{l+1}, \overline{a}_{l+2}, \ldots) \in Z_b^{\infty}$ is equal for every integer in M and $\#\{(\overline{a}_0, \ldots, \overline{a}_{l-1}) : z \in M\} = \#M = b^l$. (i.e., M is the equivalent of a b-adic block, in negative b-adic integers).

P r o o f. The first part is easily verified by simply adding $\tau_k(n)$ and $\tau_k(-n)$ (i.e., insert the given representation for $-n$) and observing that the sum, b^k, converges to 0 in the b-adic metric as k goes to infinity, while the summands converge to n and $-n$, respectively.

Regarding the second part, first note that for n in the given range we always have $r = r(n) \leq l$ and $r = l$ iff $n = (k+1)b^l$. We denote the b-adic expansion (or representation) of k by $k = \sum_{i \geq 0} k_{i+l} b^i$.

For $r < l$, it is evident that the digits of all n in the given range are constant from index l onwards and in fact equal to $k_l, k_{l+1}, \ldots$ Thus the digits of $-n$ with index at least l are also constant and equal to $b-1-k_l, b-1-k_{l+1}, \ldots$ Furthermore, the mapping between the (full range of) digits of n and $-n$ is self-inverse. In particular it is injective on the first l digits. There is, however, no n with $r(n) < l$ such that all of the first l digits are 0. Therefore the statement is proved, if we can show that the remaining case, $r = l$, $n = (k+1)b^l$, maps to the zero vector in the first l digits and, more importantly, to the same trailing digits.

For this case, we set $r' \in \mathbb{N}_0$ such that

$$k_l = k_{l+1} = \cdots = k_{l+r'-1} = b-1 \neq k_{l+r'}$$

(where the case $r' = 0$ may occur if $k_l \neq b-1$). Then, obeying the carry,

$$(k+1)b^l = (k_l+1)b^l + \sum_{i>0} k_{l+i} b^{l+i} = (k_{l+r'}+1)b^{l+r'} + \sum_{i>0} k_{l+r'+i} b^{l+r'+i},$$

so the last right hand side is again a valid expansion (representation). By our proposed formula this maps to

$$\big(b - (k_{l+r'}+1)\big)b^{l+r'} + \sum_{i>0} (b-1-k_{l+r'+i}) b^{l+r'+i} = \sum_{i \geq 0} (b-1-k_{l+i}) b^{l+i},$$

giving the desired form and concluding the argument. □

3. Relations between Algorithms 1 and 2

Theorem 1. *Let s be a dimension, $R = \mathbb{F}_q$ be a finite field with cardinality q, and $C^{(1)}, \dots, C^{(s)} \in \mathbb{F}_q^{\mathbb{N}\times\mathbb{N}_0}$ be finite-row generating matrices. Let $(s_n)_{n\geq 0}$ be a uniformly distributed sequence in $\mathbb{Z}_q$.*

If $C^{(1)}, \dots, C^{(s)}$ generate a uniformly distributed sequence via Algorithm 1, then Algorithm 2 based on these matrices and the sequence $(s_n)_{n\geq 0}$ gives a uniformly distributed sequence in $[0,1]^s$.

Proof. To prove the uniform distribution we show that every elementary interval contains the correct portion of points in the limit. Let

$$I = \prod_{i=1}^{s} \left[\frac{a_i}{q^{d_i}}, \frac{a_i+1}{q^{d_i}}\right)$$

with nonnegative integers $d_1, \dots, d_s$ (not all zero) and $a_1 < q^{d_1}, \dots, a_s < q^{d_s}$. The finite-row property ensures that there exists an L such that $c_{j,r}^{(i)} = 0$ for all $i = 1, \dots, s$, $1 \leq j \leq d_i$ and $r \geq L$. Hence $\tau_L(s_n)$ determines whether $\boldsymbol{x}_n$ of Algorithm 2 is included in I or not. Since Condition 2 holds true we know that exactly $q^{L-(d_1+\cdots+d_s)}$ residue classes $r_1, \dots, r_{q^{L-(d_1+\cdots+d_s)}}$ modulo q^L correspond to the elementary interval I. The uniform distribution of $(s_n)_{n\geq 0}$ in $\mathbb{Z}_q$ ensures that $\big(\tau_L(s_n)\big)_{n\geq 0}$ is uniformly distributed modulo q^L. Therefore,

$$\begin{aligned}
&\frac{A(N;I)}{N} - \lambda(I) \\
&= \frac{1}{N} \sum_{k=1}^{q^{L-(d_1+\cdots+d_s)}} \#\left\{0 \leq n < N : \tau_L(s_n) \equiv r_k \pmod{q^L}\right\} - \frac{1}{q^{d_1+\cdots+d_s}}
\end{aligned}$$

and thus

$$\lim_{N\to\infty} \left(\frac{A(N;I)}{N} - \lambda(I)\right) = q^{L-(d_1+\cdots+d_s)} \frac{1}{q^L} - \frac{1}{q^{d_1+\cdots+d_s}} = 0. \qquad \square$$

The converse of Theorem 1 is not true. Let $s_n = n^2$, then the sequence $(s_n)_n \geq 0$ is not uniformly distributed in $\mathbb{Z}_q$ by Example 1. But the one-dimensional sequence generated by the finite-row matrix

$$C^{(1)} = \begin{pmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & \dots & \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & \dots & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{pmatrix} \in \mathbb{F}_2^{\mathbb{N}\times\mathbb{N}_0}$$

via Algorithm 2 is a uniformly distributed digital sequence in base 2 (see [11]).

In the next theorem, we will find conditions on the generating matrices such that the uniform distribution of $(s_n)_{n\geq 0}$ is sufficient and necessary for the uniform distribution of the digital sequence. For stating the next result we introduce the term *optimal row-lengths* for the generating matrices. Let

$$C_1, \ldots, C_s \in \mathbb{F}_q^{\mathbb{N}\times\mathbb{N}_0}$$

be finite-row generating matrices. We measure the length of a row $\boldsymbol{c}_j^{(i)}$ by

$$\sup\left\{r \in \mathbb{N}_0 : c_{j,r}^{(i)} \neq 0\right\} + 1.$$

In [10] it was shown that the uniform distribution of the sequence implies that for every j there exists $i \in \{1, \ldots, s\}$ such that the length of $\boldsymbol{c}_j^{(i)}$ is at least sj. Therefore, we say that $C_1, \ldots, C_s \in \mathbb{F}_q^{\mathbb{N}\times\mathbb{N}_0}$ have *optimal row-lengths* if for all $i \in \{1, \ldots, s\}$, $j \geq 1$ the length of $\boldsymbol{c}_j^{(i)}$ is *at most* sj.

Theorem 2. *Let $s > 0$, $R = \mathbb{F}_q$ be a finite field with cardinality q, and $C^{(1)}, \ldots$ $\ldots, C^{(s)} \in \mathbb{F}_q^{\mathbb{N}\times\mathbb{N}_0}$ be finite-row generating matrices having optimal row-lengths and yielding a $(\mathbf{T}, s)$-sequence with optimal quality parameter $\mathbf{T} \equiv 0$ via Algorithm 1. Let $(s_n)_{n\geq 0}$ be a sequence in $\mathbb{Z}_q$. Then Algorithm 2 produces a uniformly distributed sequence if and only if $(s_n)_{n\geq 0}$ is uniformly distributed in $\mathbb{Z}_q$.*

Proof. Sufficiency of the uniform distribution of $(s_n)_{n\geq 0}$ in $\mathbb{Z}_q$ follows from Theorem 1. To prove necessity we regard elementary intervals of the following form

$$I = \prod_{i=1}^{s} \left[\frac{a_i}{q^d}, \frac{a_i+1}{q^d}\right), \tag{4}$$

where $d \in \mathbb{N}$ and $0 \leq a_i < q^d$ for $i = 1, \ldots, s$. We denote the base q representation of $\frac{a_i}{q^d}$ by

$$\frac{a_i}{q^d} = \frac{a_{i,1}}{q} + \frac{a_{i,2}}{q^2} + \cdots + \frac{a_{i,d}}{q^d}$$

and the q-adic representation of s_n, for some fixed n, by

$$s_n = \sum_{r=0}^{\infty} \overline{a}_r q^r.$$

The optimal row-lengths yield the equivalence of $\boldsymbol{x}_n \in I$ and

$$\underbrace{\begin{pmatrix} c_{1,0}^{(1)} & \cdots & c_{1,ds-1}^{(1)} \\ \vdots & & \vdots \\ c_{d,0}^{(1)} & \cdots & c_{d_1,ds-1}^{(1)} \\ \vdots & & \vdots \\ c_{1,0}^{(s)} & \cdots & c_{1,ds-1}^{(s)} \\ \vdots & & \vdots \\ c_{d,0}^{(s)} & \cdots & c_{d_s,ds-1}^{(s)} \end{pmatrix}}_{:=\overline{C}} \begin{pmatrix} \psi_0(\overline{a}_0) \\ \vdots \\ \psi_{ds-1}(\overline{a}_{ds-1}) \end{pmatrix} = \begin{pmatrix} \lambda_{1,1}^{-1}(a_{1,1}) \\ \vdots \\ \lambda_{1,d_1}^{-1}(a_{1,d}) \\ \vdots \\ \lambda_{s,1}^{-1}(a_{s,1}) \\ \vdots \\ \lambda_{s,d_s}^{-1}(a_{s,d}) \end{pmatrix} \in \mathbb{F}_q^{ds},$$

with the maps $\psi_i, \lambda_{i,j}$ of Algorithm 1. Note that $\overline{C}$ is a square matrix with full row-rank ds, and that there are q^{ds} elementary intervals of the form (4) which are in one to one correspondence with the elements in $\mathbb{F}_q^{ds}$. Further, note that the value of $\tau_{sd}(s_n)$ determines whether $\boldsymbol{x}_n$ is included in I or not. Now the uniform distribution of $(\boldsymbol{x}_n)_{n\geq 0}$ ensures that $\big(\tau_{sd}(s_n)\big)_{n\geq 0}$ is uniformly distributed modulo q^{sd}. Since this is valid for every $d \in \mathbb{N}$, we have that $\big(\tau_k(s_n)\big)_{n\geq 0}$ is uniformly distributed modulo q^k for every $k \in \mathbb{N}$ (clearly, uniform distribution propagates to lower powers). Finally by Lemma 1, this is equivalent to $(s_n)_{n\geq 0}$ being uniformly distributed in $\mathbb{Z}_q$. □

Example 2. Constructions and examples of generating matrices having optimal row-lengths and satisfying Condition 1 for $\mathbf{T} \equiv 0$ are given, e.g., in [6, 10, 13].

One specific example of suitable matrices are the Stirling matrices, constructed in analogy to the classical Pascal or Faure matrices but with Stirling numbers of the first kind replacing the binomials. Here are depicted matrices in base 5 (see Figure 1). The finite row length is clearly visible. The apparent fractal structure and other aspects are explored in more detail in [13].

Figure 1. Matrices in base 5.

Remark 1. Theorem 2 in case of $s = 1$ and $C^{(1)}$ chosen to be the identity matrix represents a generalization of the one-dimensional case of [5, Theorem 4.2.(iv)].

4. Discrepancy and quality-parameter function T for Algorithm 2 using some specific $(s_n)_{n\geq 0}$

The probably most basic setting for $(s_n)_{n\geq 0}$ is to choose $s_n = n$. Trivially, in this case Condition 1 is also qualified to determine the quality parameter or function, t or $\mathbf{T}$, respectively, of the sequence constructed by Algorithm 2. Next, we look at negative integers as the underlying sequence.

Proposition 1 (The case $s_n = -n-1$). Let s be a dimension, q be a prime power, $R = \mathbb{F}_q$, and $C^{(1)}, \ldots, C^{(s)} \in \mathbb{F}_q^{\mathbb{N}\times\mathbb{N}_0}$ be finite-row generating matrices.

If $C^{(1)}, \ldots, C^{(s)}$ generate a $(\mathbf{T}, s)$-sequence in base q via Algorithm 1, then Algorithm 2 based on these matrices and the sequence $(s_n)_{n\geq 0} = (-n-1)_{n\geq 0}$ gives a $(\mathbf{T}, s)$-sequence in base q.

P r o o f. Let k, m be any nonnegative integers such that $\mathbf{T}(m) < m$. We have to prove that $[\boldsymbol{x}_n]_{q,m}$ with $n = kb^m$, $kb^m+1, \ldots, kb^m+b^m-1$ forms a $\big(\mathbf{T}(m), m, s\big)$--net in base q. We regard an elementary interval of the form

$$I = \prod_{i=1}^{s} \left[\frac{a_i}{q^{d_i}}, \frac{a_i+1}{q^{d_i}}\right)$$

with integers

$$d_i \geq 0, \quad 0 \leq a_i < q^{d_i} \quad \text{for} \quad i = 1, \ldots, s \quad \text{satisfying} \quad d_1 + \cdots + d_s = m - \mathbf{T}(m).$$

We use the base q digit expansion

$$a_i/q^{d_i} = \sum_{j=1}^{d_i} \frac{a_{i,j}}{q^j}.$$

Regarding Algorithm 2 we see that $[\boldsymbol{x}_n]_{q,m} \in I$ (for some fixed n) if and only if

$$\begin{pmatrix} c_{1,0}^{(1)} & c_{1,1}^{(1)} & \cdots \\ \vdots & \vdots & \\ c_{d_1,0}^{(1)} & c_{d_1,1}^{(1)} & \cdots \\ \vdots & \vdots & \\ c_{1,0}^{(s)} & c_{1,1}^{(s)} & \cdots \\ \vdots & \vdots & \\ c_{d_s,0}^{(s)} & c_{d_s,1}^{(s)} & \cdots \end{pmatrix} \begin{pmatrix} \psi_0(\overline{a}_0) \\ \psi_1(\overline{a}_1) \\ \vdots \end{pmatrix} = \begin{pmatrix} \lambda_{1,1}^{-1}(a_{1,1}) \\ \vdots \\ \lambda_{1,d_1}^{-1}(a_{1,d_1}) \\ \vdots \\ \lambda_{s,1}^{-1}(a_{s,1}) \\ \vdots \\ \lambda_{s,d_s}^{-1}(a_{s,d_s}) \end{pmatrix},$$

where we used the notation $-n-1 = \sum_{r=0}^{\infty} \overline{a}_r q^r$. Equivalently,

$$\begin{pmatrix} c_{1,0}^{(1)} & \cdots & c_{1,m-1}^{(1)} \\ \vdots & & \vdots \\ c_{d_1,0}^{(1)} & \cdots & c_{d_1,m-1}^{(1)} \\ \vdots & & \vdots \\ c_{1,0}^{(s)} & \cdots & c_{1,m-1}^{(s)} \\ \vdots & & \vdots \\ c_{d_s,0}^{(s)} & \cdots & c_{d_s,m-1}^{(s)} \end{pmatrix} \begin{pmatrix} \psi_0(\overline{a}_0) \\ \vdots \\ \psi_{m-1}(\overline{a}_{m-1}) \end{pmatrix}$$

$$= \begin{pmatrix} \lambda_{1,1}^{-1}(a_{1,1}) \\ \vdots \\ \lambda_{1,d_1}^{-1}(a_{1,d_1}) \\ \vdots \\ \lambda_{s,1}^{-1}(a_{s,1}) \\ \vdots \\ \lambda_{s,d_s}^{-1}(a_{s,d_s}) \end{pmatrix} - \begin{pmatrix} c_{1,m}^{(1)} & c_{1,m+1}^{(1)} & \cdots \\ \vdots & \vdots & \\ c_{d_1,m}^{(1)} & c_{d_1,m+1}^{(1)} & \cdots \\ \vdots & \vdots & \\ c_{1,m}^{(s)} & c_{1,m+1}^{(s)} & \cdots \\ \vdots & \vdots & \\ c_{d_s,m}^{(s)} & c_{d_s,m+1}^{(s)} & \cdots \end{pmatrix} \begin{pmatrix} \psi_m(\overline{a}_m) \\ \psi_{m+1}(\overline{a}_{m+1}) \\ \vdots \end{pmatrix}.$$

Lemma 3 ensures that all terms on the right hand side are independent of n for the range $n = kb^m, kb^m+1, \ldots, kb^m+b^m-1$ and also that the vector on the left hand side spans $\mathbb{F}_q^m$ as n ranges through $n = kb^m, kb^m+1, \ldots, kb^m+b^m-1$. Since Condition 1 holds we know that the system has exactly $q^{m-\mathbf{T}(m)}$ solutions for $n = kb^m, kb^m+1, \ldots, kb^m+b^m-1$. □

Proposition 1 immediately implies the following corollary.

Corollary 1 (The case $s_n = (-1)^n\lfloor(n+1)/2\rfloor$)**.** *Let s be a dimension, q be a prime power, $R = \mathbb{F}_q$, and $C^{(1)}, \ldots, C^{(s)} \in \mathbb{F}_q^{\mathbb{N}\times\mathbb{N}_0}$ be finite-row generating matrices.*

If $C^{(1)}, \ldots, C^{(s)}$ generate a $(\mathbf{T}, s)$-sequence in base q via Algorithm 1, then Algorithm 2 with the same matrices and the underlying sequence

$$(s_n)_{n\geq 0} = \big((-1)^n\lfloor\frac{n+1}{2}\rfloor\big)_{n\geq 0}$$

produces a sequence, where the two subsequences $(\boldsymbol{x}_{2n})_{n\geq 0}$ and $\big(\boldsymbol{x}_{2n+1}\big)_{n\geq 0}$ are $(\mathbf{T}, s)$-sequences in base q.

For stating the next result we introduce the magnitude $\Delta_b(t,m,s)$, which is defined to be an upper bound for $D_N^*(\mathcal{P})$ holding for every (t,m,s)-net $\mathcal{P}$ in base b

$$b^m D_{b^m}^*(\mathcal{P}) \le \Delta_b(t,m,s).$$

In this paper we do not aim to give the most precise estimate but include for the sake of completeness exemplarily the well-known bound of Niederreiter for $b > 2$ (see [24, Theorem 4.5])

$$\Delta_b(t,m,s) = b^t \sum_{i=0}^{s-1} \binom{s-1}{i} \binom{m-t}{i} \left\lfloor \frac{b}{2} \right\rfloor^i.$$

Proposition 2 (The case $s_n = n+\alpha$)**.** Let s be a dimension, q be a prime power, $R = \mathbb{F}_q$, and $C^{(1)}, \dots, C^{(s)} \in \mathbb{F}_q^{\mathbb{N}\times\mathbb{N}_0}$ be finite-row generating matrices satisfying the quality parameter function $\mathbf{T} : \mathbb{N}_0 \to \mathbb{N}_0$ in Condition 1. Furthermore, let α be a p-adic integer with representation

$$\alpha = \sum_{i=0}^{\infty} a_i q^i \quad \text{and set} \quad (s_n)_{n\ge 0} = (n+\alpha)_{n\ge 0}.$$

Then the discrepancy of the first N points of the sequence $\mathcal{S}$ produced by Algorithm 2 satisfies

$$\begin{aligned} N D_N(\mathcal{S}) &\le (q-a_0)\Delta_q\big(\mathbf{T}(0),0,s\big) \\ &\quad + \sum_{j=1}^{r-1}(q-1-a_j)\Delta_q\big(\mathbf{T}(j),j,s\big) + \sum_{j=0}^{r} b_j \Delta_q\big(\mathbf{T}(j),j,s\big), \end{aligned}$$

where $r = \lfloor \log_q(N) \rfloor$ and $\sum_{j=0}^{r} b_j q^j$ is the base q representation of

$$N' = N - q^r + \sum_{j=0}^{r-1} a_j q^j.$$

P r o o f. First collect the digits a_j with $1 \le j \le r-1$ of α satisfying $a_j \ne q-1$ and denote them by $a_{k(1)}, a_{k(2)}, \dots, a_{k(j')}$, where $1 \le k(1) < k(2) < \dots < k(j') \le r-1$ and j' is the number of such digits. Observe that

$$q^r - \sum_{i=0}^{r-1} a_i q^i = q - a_0 + \sum_{i=1}^{j'} \big(q-1-a_{k(i)}\big) q^{k(i)}.$$

Bearing in mind the basic fact that if dividing a point set $\mathcal{P}$ of N points into l disjoint sets $\mathcal{P}_1$ with N_1 points, …, $\mathcal{P}_l$ with N_l points, then

$$N D_N(\mathcal{P}) \le \sum_{w=1}^{l} N_w D_{N_w}(\mathcal{P}_w)$$

— we divide the first $q^r - \sum_{i=0}^{r-1} a_i q^i$ points as follows.

We start with the first $q - a_0$ points which are obviously $q - a_0$ instances of $\big(T(0), 0, s\big)$-nets in base q.

For the next step we observe that the q-adic expansions of the next $q^{k(1)}$ points have all equal digits at position $k(1)$ and larger, and the digits at positions 0 to $k(1) - 1$ span $\{0, 1, \ldots, q - 1\}^{k(1)}$. Hence they form via Algorithm 2 a $\big(T\big(k(1)\big), k(1), s\big)$-net in base q. We have n in the range

$$q - a_0, q - a_0 + 1, \ldots, q - a_0 + q^{k(1)} - 1$$

and thus $n + \alpha$ of the form

$$A_1, 1 + A_1, \ldots, q^{k(1)} - 1 + A_1$$

with $A_1 := \big(a_{k(1)} + 1\big)q^{k(1)} + \sum_{i=k(1)+1}^{\infty} a_i q^i$. Now analogous argumentation as in the proof of Proposition 1 imply that these $q^{k(1)}$ points form a $\big(\mathbf{T}(k(1)), k(1), s\big)$--net in base q. Altogether we obtain step by step $(q - 1 - a_{k(1)})$ nets of this form. Absolutely identically we obtain $q - 1 - a_{k(2)}$, $\big(\mathbf{T}(k(2)), k(2), s\big)$-nets in base $q, \ldots,$ and $q - 1 - a_{k(j')}$, $\big(\mathbf{T}(k(j')), k(j'), s\big)$-nets in base q. This explains the first two terms in the upper bound.

It remains to estimate the discrepancy of the residual $N' = N - q^r + \sum_{j=0}^{r-1} a_j q^j$ points. We denote the base q representation of N' by $N' = \sum_{j=0}^{r} b_j q^j$. Now we collect the digits b_j with $1 \le j \le r$ of N' satisfying $b_j \neq 0$ and denote them by $b_{k(1)}, b_{k(2)}, \ldots, b_{k(j'')}$, where $1 \le k(1) < k(2) < \ldots < k(j'') \le r$, and j'' is the number of such digits.

We regard the next $q^{k(j'')}$ points, i.e., n in the range

$$q^r - \sum_{i=0}^{r-1} a_i q^i, q^r - \sum_{i=0}^{r-1} a_i q^i + 1, \ldots, q^r - \sum_{i=0}^{r-1} a_i q^i + q^{k(j'')-1}.$$

Now adding α yields

$$A_2, 1 + A_2, \ldots, q^{k(j'')} - 1 + A_2,$$

where $A_2 := (a_r + 1)q^r + \sum_{i=r+1}^{\infty} a_i q^i$. As above the b-adic digits for powers with exponents at least $k(j'')$ are fixed and the first $k(j'')$ digits span $\{0, 1, \ldots \ldots, q - 1\}^{k(j'')}$. Hence those point sets form a $\big(T(k(j'')), k(j''), s\big)$-net in base q.

Step by step we obtain $b_{k(j'')}$ such nets and we obtain the first summand in the second sum of the theorem. Again, step by step, we obtain the last sum of the upper bound. □

Corollary 2. *If, furthermore,* $\mathbf{T}(m) \le t$ *with* $t \in \mathbb{N}_0$ *in Proposition 2, then* $\mathcal{S}$ *is a low-discrepancy sequence.*

P r o o f. In this case we have $\Delta_q(t,j,s) \le c_{q,s,t} j^{s-1} + \mathcal{O}(j^{s-2})$ for all $j \ge 0$, where the implied constant is independent of j. (See [3] for the best known constant $c_{q,s,t}$.) Using this bound in the upper bound of Proposition 2 we obtain the desired result $ND_N(\mathcal{S}) = O((\log N)^s)$. □

Corollary 3 ($s_n = \frac{1}{v}n + \alpha$). *Let s be a dimension, q be a prime power, t be a nonnegative integer, $R = \mathbb{F}_q$, and $C^{(1)}, \ldots, C^{(s)} \in \mathbb{F}_q^{\mathbb{N}\times\mathbb{N}_0}$ be finite-row generating matrices satisfying the quality parameter function $\mathbf{T} \equiv t$ in Condition 1. Furthermore, let α be a p-adic integer and $v \in \mathbb{N}$ satisfying* $\gcd(v,q) = 1$. *Set $(s_n)_{n\ge0} = (\frac{1}{v}n + \alpha)_{n\ge0}$. Then the sequence $\mathcal{S}$ produced by Algorithm 2 is a low-discrepancy sequence.*

P r o o f. The strategy is to split the sequence into v subsequences

$$\left(s_n^{(1)}\right)_{n\ge0}, \left(s_n^{(2)}\right)_{n\ge0}, \ldots, \left(s_n^{(v)}\right)_{n\ge0}$$

of the form

$$\begin{aligned} s_n^{(1)} &= n + \alpha =: n + \alpha_1, \\ s_n^{(2)} &= n + \frac{1}{v} + \alpha =: n + \alpha_2, \\ &\vdots \\ s_n^{(v)} &= n + \frac{(v-1)}{v} + \alpha =: n + \alpha_v. \end{aligned}$$

Since $\gcd(q,v) = 1$, all of the fractions and thus all of $\alpha_1, \alpha_2, \ldots, \alpha_v$ are q-adic integers. Then all v subsequences are low-discrepancy sequences by Corollary 2 and the result follows. □

Remark 2. Previously, subsequences of digital sequences produced by Algorithm 1 have been investigated, see, e.g., [8, 9, 11, 15]. In particular, subsequences indexed by arithmetic progressions were discussed in [8, 9]. Unfortunately, the discrepancy of such sequences is a difficult subject and there exist negative results such as [8, Example 5]. Hence the obvious generalization of Corollary 3 to $s_n = \frac{u}{v}n + \alpha$ would be a difficult task as well.

5. Numerical Experiments and Discussion

The following plots give a comparison between three different input sequences:

- first, the classical sequence $s_n = n$,
- then the alternating sequence $s_n = (-1)^n \lfloor (n+1)/2 \rfloor$ and
- finally, the sequence $s_n = (2n-1)/4$ in $\mathbb{Z}_5$.

The generating matrices are the first two Stirling matrices in base 5 seen in Example 2 and the number of points is 500.

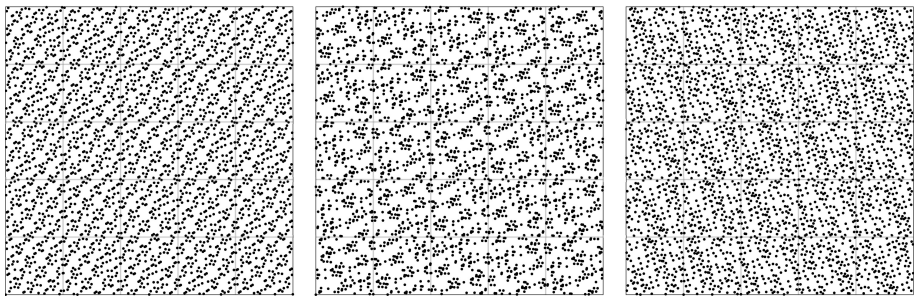

FIGURE 2. A comparison between three different input sequences.

We have also calculated explicitly the star discrepancy for some newly constructed sequences. We found similar asymptotic behavior to the classical constructions but with an improvement in the constants. In Figure 3 we look at one-dimensional sequences constructed with the identity matrix over $\mathbb{F}_2$ and used as input sequences in $\mathbb{Z}_2$:

$s_n = n$ (black line),

$s_n = (-1)^n \lfloor (n+1)/2 \rfloor$ (gray line), and

$s_n = n - 2/5$ (blue line).

We graphed the star discrepancy of the first N points, divided by the asymptotic $\log N/N$, and smoothed it by a moving average over ten points. The improvement in the constant can be clearly observed and, therefore, it is an interesting topic for future research. Furthermore, it is interesting to note that the construction corresponding to the gray line also describes the symmetrized binary van der Corput sequence. Symmetrization has been shown to improve the asymptotic behavior of the L_p-discrepancy [16].

We also computed the star discrepancy for two dimensional sequences constructed with the Stirling matrices over $\mathbb{F}_2$ (see [13]) in Figure 4. Here we used as input sequences:

$s_n = n$ (black line),

$s_n = -n - 1$ (gray line), and

$s_n = n - 2^{10}/(2^{11} + 1)$ (dashed blue line) in $\mathbb{Z}_2$.

As in the one-dimensional case, we divided by the asymptotic ($\log^2 N/N$) and smoothed the graph by a moving average over ten points. Again we observe an improvement in the constants.

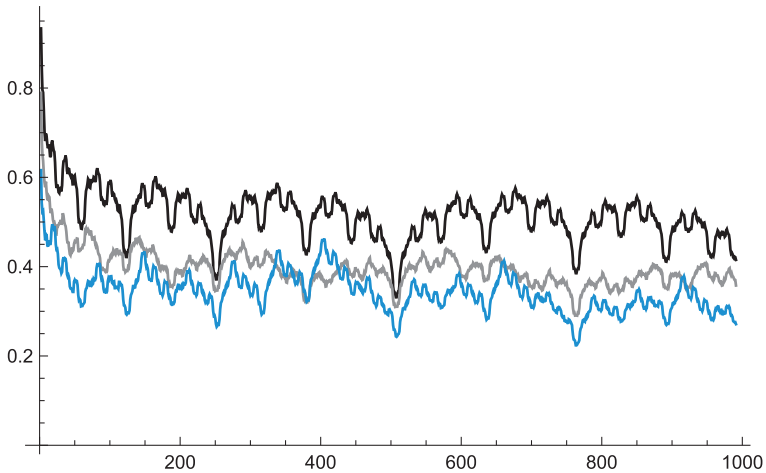

FIGURE 3. One-dimensional sequences constructed with the identity matrix over $\mathbb{F}_2$.

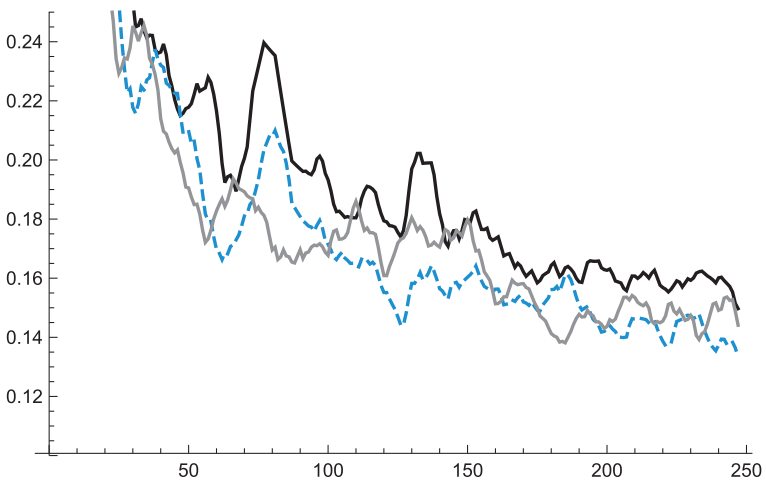

FIGURE 4. Two dimensional sequences constructed with the Stirling matrices over $\mathbb{F}_2$.

In both cases we found that a b-adic shift closed to $-1/b$ shows good results and might be interesting for forthcoming investigations. For instance, this might be a good explicit candidate for the b-adic shift of the Halton sequence which were studied, for example, in [4].

Acknowledgements. We would like to thank the anonymous referees, whose suggestions helped to improve the quality of the paper. The first author is supported by the Austrian Science Fund (FWF): Project F5505-N26, which is a part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications", the second by the Austrian Science Fund (FWF): Project F5511-N26, which is a part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications" as well as Project P27351-N26.

REFERENCES

[1] BUNDSCHUH, P.—ZHU Y. C.: *A method for exact calculation of the discrepancy of low-dimensional point sets*, Abh. Math. Sem. Univ. Hamburg **63** (1993), 115–133.

[2] DICK, J.—PILLICHSHAMMER, F.: *Digital Nets and Sequences. Discrepancy Theory and Quasi-Monte Carlo Integration.* Cambridge University Press, Cambridge, 2010.

[3] FAURE, H.—KRITZER, P.: *New star discrepancy bounds for* (t, m, s)*-nets and* (t, s)*--sequences*, Monatsh. Math. **172** (2013), 55–75.

[4] HELLEKALEK, P.—KRITZER, P.—PILLICHSHAMMER, F.: *Open type quasi-Monte Carlo integration based on Halton sequences in weighted Sobolev spaces*, J. Complexity **33** (2016), 169–189.

[5] HELLEKALEK, P.—NIEDERREITER, H.: *Constructions of uniformly distributed sequences using the b-adic method*, Unif. Distrib. Theory **6** (2011), no. 1, 185–200.

[6] HOFER, R.: *A construction of digital* $(0, s)$*-sequences involving finite-row generator matrices*, Finite Fields Appl. **18** (2012), 587–596.

[7] HOFER, R.: *A construction of low-discrepancy sequences involving finite-row digital* (t, s)*-sequences*, Monatsh. Math. **171** (2013), 77–89.

[8] ——— *On sbsequences of Niederreiter-Halton sequences.* In: Monte Carlo and Quasi-Monte Carlo Methods 2008. (P. L'Ecuyer, A. B. Owen, eds.), Springer-Verlag, Berlin, 2009, pp. 423–438.

[9] HOFER, R.—KRITZER, P.—LARCHER, G.—PILLICHSHAMMER, F.: *Distribution properties of generalized van der Corput-Halton sequences and their subsequences*, J. Number Theory **5** (2009), no. 4, 719–746.

[10] HOFER, R.—LARCHER, G.: *On existence and discrepancy of certain digital Niederreiter-Halton sequences*, Acta Arith. **141** (2010), no. 4, 369–394.

[11] HOFER, R.—LARCHER, G.—ZELLINGER, H.: *On the Digits of Squares and the Distribution of Quadratic Subsequences of Digital Sequences*, Proceedings of Amer. Math. Sci. **141** (2012), no. 5, 1551–1565.

[12] HOFER, R.—NIEDERREITER, H.: *A construction of (t,s)-sequences with finite-row generating matrices using global function fields*, Finite Fields Appl. **21** (2013), 97–110.

[13] HOFER, R.—PIRSIC, G.: *An explicit construction of finite-row digital* $(0, s)$*-sequences*, Unif. Distrib. Theory **6** (2011), no. 2, 13–30.

[14] ——— *A finite-row scrambling of Niederreiter sequences*, In: Monte Carlo and Quasi--Monte Carlo Methods 2012. (J.Dick F. Y. Kuo, G. W. Peters I. H. Sloan, eds.) Springer Proceedings in Mathematics & Statistics (PROMS, Vol. 65), Springer-Verlag, 2013, pp. 427–437.

[15] HOFER, R.—ZELLINGER, H.: *Distribution Properties of Certain Subsequences of Digital Sequences and Their Hybrid Version*, Unif. Distrib. Theory **8** (2013), no. 2, 121–140.

[16] KRITZINGER, R.—PILLICHSHAMMER, F.: *L_p-discrepancy of the symmetrized van der Corput sequence*, Arch. Math. **105** (2015), no. 5, 407–418.

[17] KUIPERS, L.—NIEDERREITER, H.: *Uniform Distribution of Sequences*. Wiley, New York, 1974.

[18] LARCHER, G.—NIEDERREITER, H.: *Generalized (t,s)-sequences, Kronecker-type sequences, and Diophantine approximations of formal Laurent series*, Trans. Amer. Math. Soc. **347** (1995), no. 6, 2051–2073.

[19] MAHLER, K.: *p-adic Numbers and their Functions* (2nd edition). Cambridge University Press, Cambridge, 1981.

[20] MEIJER, H. G.: *Uniform distribution of g-adic integers*, Nederl. Akad. Wetensch. Proc. Ser. **A 70**=Indag. Math. **29** (1967), 535–546.

[21] MEIJER, H. G.—SHIUE, J. S.: *Uniform distribution in $\mathbb{Z}_g$ and $\mathbb{Z}_{g_1} \times \cdots \times \mathbb{Z}_{g_t}$*, Indag. Math. **79** (1976), 200–212.

[22] NIEDERREITER, H.: *Discrepancy and convex programming*, Ann. Mat. Pura Appl. **93** (1972), 89–97.

[23] ——— *Point sets and sequences with small discrepancy*, Monatsh. Math. **104** (1987), no. 4, 273–337.

[24] ——— *Random Number Generation and Quasi-Monte Carlo Methods*. In: CBMS-NSF Regional Conference Series in Applied Mathematics Vol. 63, SIAM, Philadelphia, 1992.

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

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

[27] ——— *A construction of low-discrepancy sequences using global function fields*, Acta Arith. **73** (1995), 87–102.

[28] TEZUKA, S.: *Polynomial arithmetic analogue of Halton sequences*, ACM Trans. Model. Comput. Simulation **3** (1993), 99–107.

Received June 19, 2017
Accepted November 21, 2017

Roswitha Hofer,
Ísabel Pirsic
Institute of Financial Mathematics and
Applied Number Theory
Johannes Kepler University Linz
Altenbergerstr. 69
A-4040 Linz
AUSTRIA
E-mail: roswitha.hofer(at)jku.at, isabel.pirsic(at)jku.at