ACTA ARITHMETICA
141.4 (2010)

On existence and discrepancy of certain digital Niederreiter–Halton sequences

by

Roswitha Hofer and Gerhard Larcher (Linz)

1. Introduction. The concept of digital (t,s)-sequences in the sense of Niederreiter (see e.g. [11]) or—more general—of digital $(\mathbf{T},s)$-sequences (see [9]) is the most powerful technique to construct low-discrepancy point sequences in an s-dimensional unit cube.

By a *low-discrepancy sequence* in $[0,1)^s$ we mean a sequence $(\boldsymbol{x}_n)_{n\geq 0}$ such that discrepancy D_N^* of the first N elements of the sequence satisfies

$$D_N^* = O((\log N)^s/N),$$

where

$$D_N^* = D_N^*(\boldsymbol{x}_0,\ldots,\boldsymbol{x}_{N-1}) := \sup_{B\subseteq[0,1)^s} |A_N(B)/N - \lambda(B)|,$$

where $A_N(B)$ denotes $\#\{n \mid 0 \leq n < N,\ \boldsymbol{x}_n \in B\}$ and the supremum is extended over all sub-boxes B of $[0,1)^s$ of the form $B = \prod_{i=1}^s [0,a_i)$ with $0 < a_i \leq 1$ for $i \in \{1,\ldots,s\}$.

A sequence is called *uniformly distributed* if $\lim_{N\to\infty} D_N^* = 0$. It is a famous conjecture that $(\log N)^s/N$ is the best possible order for the discrepancy of a sequence in $[0,1)^s$. (An excellent introduction into the theory of uniform distribution can be found in the book of Kuipers and Niederreiter [8] or in the book of Drmota and Tichy [1].)

We give the definition of digital $(\mathbf{T},s)$-sequences.

Definition 1. Let s be a dimension and q be a prime. Let $C_1,\ldots,C_s$ be $\mathbb{N}\times\mathbb{N}$-matrices in the finite field $\mathbb{Z}_q$. We construct a sequence $(\boldsymbol{x}_n)_{n\geq 0}$, $\boldsymbol{x}_n = (x_n^{(1)},\ldots,x_n^{(s)})$, $n \in \mathbb{N}_0$, by generating the ith coordinate of the nth point, $x_n^{(i)}$, as follows. Represent $n = n_0 + n_1 q + n_2 q^2 + \cdots$ in base q. Then

2010 *Mathematics Subject Classification*: 11K06, 11K31, 11K38.
Key words and phrases: discrepancy, low-discrepancy sequences, Halton sequences, digital $(\mathbf{T},s)$-sequences, Niederreiter–Halton sequences.

DOI: 10.4064/aa141-4-5

set

$$C_i \cdot (n_0, n_1, \dots)^\top =: (y_0^{(i)}, y_1^{(i)}, \dots)^\top \in \mathbb{Z}_q^{\mathbb{N}}$$

and

$$x_n^{(i)} := \frac{y_0^{(i)}}{q} + \frac{y_1^{(i)}}{q^2} + \cdots .$$

For every $m \in \mathbb{N}$ let $\mathbf{T}(m)$, satisfying $0 \leq \mathbf{T}(m) \leq m$, be such that for all $d_1, \dots, d_s \in \mathbb{N}_0$ with $d_1 + \cdots + d_s = m - \mathbf{T}(m)$ the $(m - \mathbf{T}(m)) \times m$-matrix consisting of

the upper left $d_1 \times m$-submatrix of C_1 together with
the upper left $d_2 \times m$-submatrix of C_2 together with
$\vdots$
the upper left $d_s \times m$-submatrix of C_s

has rank $m - \mathbf{T}(m)$. Then $(\boldsymbol{x}_n)_{n \geq 0}$ is called a *digital* $(\mathbf{T}, s)$*-sequence* over $\mathbb{Z}_q$. If $\mathbf{T}$ is minimal with this property, we speak of a *strict digital* $(\mathbf{T}, s)$*-sequence*.

A strict digital $(\mathbf{T}, s)$-sequence is uniformly distributed if and only if $\lim_{m\to\infty}(m - \mathbf{T}(m)) = +\infty$. If $\mathbf{T}(m) \leq t$ for all m, then we speak of a *digital* (t, s)*-sequence* and we know that such sequences are low-discrepancy sequences.

The O-constant in the (low-) discrepancy estimate is—generally speaking—smaller for smaller t (≥ 0).

In searching for further classes of uniformly distributed or even low-discrepancy point sets, a method near at hand is to combine v different digital $(\mathbf{T}_i, w_i)$-sequences in different prime bases $q_1, \dots, q_v$ with $w_1 + \cdots + w_v = s$ into a single sequence in $[0,1)^s$.

A basic example is the Halton sequence which is a combination of s digital $(0,1)$-sequences in different prime bases $q_1, \dots, q_s$ generated by the unit matrices in $\mathbb{Z}_{q_i}$ for each i. It has long been known that the Halton sequences are low-discrepancy sequences.

Sequences of the above form will be called *Niederreiter–Halton* (NH) *sequences*. General NH sequences were first investigated in [6]. In [4] it was shown that a NH sequence is uniformly distributed if and only if each component digital $(\mathbf{T}_i, w_i)$-sequence is uniformly distributed.

It is the aim of this paper to make a first step in investigating the discrepancy of these sequences and especially to investigate if there are low-discrepancy sequences (apart from "trivial" cases) in the class of NH sequences.

A first general discrepancy estimate was given in [6] for the special class of "finite row" NH sequences. We say that a NH sequence is a *"finite row" NH sequence* if all generating matrices of the component digital

$(\mathbf{T}_i, w_i)$-sequences have "finite rows", i.e., each row contains only finitely many entries different from zero. NH sequences which are not "finite row" NH sequences will be called *"infinite row" NH sequences.*

It will turn out to be difficult to give a detailed and complete analysis of the discrepancy of NH sequences.

Further, it will turn out that quite different techniques are needed for "finite row" and "infinite row" NH sequences. Finally, for "infinite row" NH sequences in most cases we will obtain rather negative results, i.e., we will obtain non-low-discrepancy results. So searching for low-discrepancy NH sequences seems to be more promising among "finite row" NH sequences.

Here one basic problem however is: to obtain low-discrepancy NH sequences we have to combine (t_i, w_i)-sequences (i.e. with bounded $\mathbf{T}_i$). Until now the only known digital (t_i, w_i)-sequences with "finite rows" have been one-dimensional digital $(t_i, 1)$-sequences. In Theorem 4 of this paper it is shown that for every dimension s there exist "finite row" $(0, s)$-sequences. In some sense best possible explicit examples of such sequences will be given.

We start our investigations in Section 2 with a result on weighted sums of digits of multiples of 3, which in some sense generalizes a result of Newman [10] and which will be essential later on for our discrepancy analysis.

In Section 3 we state and prove our results on the discrepancy of "finite row" and "infinite row" NH sequences. In particular, we give a quite general lower bound for the discrepancy of "infinite row" NH sequences.

Finally, in Section 4 we provide the existence results and explicit constructions for "finite row" digital sequences.

2. Weighted sums of digits of arithmetic subsequences. In this section we will prove a result on the distribution of weighted sums of digits of multiples of 3 considered modulo 2. This partly generalizes a result of Newman [10] given for the unweighted sum of digits.

Definition 2. Let $\gamma := (\gamma_0, \gamma_1, \gamma_2, \ldots)$ with $\gamma_j \in \mathbb{Z}$ be a weight sequence, and $q \geq 2$ be a given base. For a non-negative integer n let $n = n_0 + n_1 q + \cdots + n_r q^r$ be the base q representation of n. Then the *weighted sum of digits* of n is defined by

$$s_{\gamma,q}(n) := n_0\gamma_0 + n_1\gamma_1 + \cdots + n_r\gamma_r.$$

It is a well-known result of Newman [10] for the unweighted sum of digits $s_2(n)$ in base $q = 2$, i.e. for $\gamma_j = 1$ for all j, that

$$\sum_{\substack{n=0 \\ n\equiv 0\,(3)}}^{N-1} (-1)^{s_2(n)} > cN^{\log 3/\log 4}$$

for some constant $c > 0$ and all N. Consequently,

$$\#\{0 \le n < N \mid n \equiv 0\ (3) \text{ and } s_2(n) \equiv 0\ (2)\} - N/6 > cN^{\log 3/\log 4}$$

for some constant $c > 0$ and all N.

We will now consider the above sum in the weighted case and for certain values of N:

$$\Pi_{m,k} := \sum_{\substack{n=0\\ n\equiv k\,(3)}}^{2^{2m+1}-1} (-1)^{s_{\gamma,2}(n)}.$$

We will show

Theorem 1.

$$\Pi_{m,0} = \begin{cases} (2^{2m+1}+1)/3 & \textit{if } \rho(2m) = 0, \\ 3^{\rho(2m)/2}\kappa & \textit{otherwise,} \end{cases}$$

where $\rho(2m) := \#\{0 \le j \le 2m \mid \gamma_j \equiv 1\ (2)\}$ *and* $\kappa \in \{\pm 1/\sqrt{3}, \pm 1/3\}$.

Proof. By the structure of the problem we can restrict to $\gamma_j \in \{0,1\}$. If $\gamma_j = 0$ for all $0 \le j \le 2m$, then

$$\sum_{\substack{n=0\\ n\equiv 0\,(3)}}^{2^{2m+1}-1} (-1)^{s_{\gamma,2}(n)} = \sum_{\substack{n=0\\ n\equiv 0\,(3)}}^{2^{2m+1}-1} 1 = \frac{2^{2m+1}+1}{3}.$$

In the following we assume that there exists at least one $j \in \{0,1,\dots,2m\}$ such that $\gamma_j = 1$. Using the relation

$$\frac{1}{q}\sum_{l=0}^{q-1} e^{2\pi i n l/q} = \begin{cases} 1 & \text{if } n \equiv 0\ (q), \\ 0 & \text{otherwise,} \end{cases}$$

we obtain

$$\begin{aligned}\sum_{\substack{n=0\\ n\equiv 0\,(3)}}^{2^{2m+1}-1} (-1)^{s_{\gamma,2}(n)} &= \frac{1}{3}\sum_{l=0}^{2}\sum_{n=0}^{2^{2m+1}-1} e^{2\pi i(3s_{\gamma,2}(n)+2ln)/6} \\ &= \frac{1}{3}\sum_{l=0}^{2}\sum_{n=0}^{2^{2m+1}-1} e^{2\pi i(s_{\overline{\gamma}^{(l)},2}(n))/6} \\ &= \frac{1}{3}\sum_{l=0}^{2}\prod_{j=0}^{2m}(1+e^{2\pi i\overline{\gamma}_j^{(l)}/6}),\end{aligned}$$

where $\overline{\gamma}_j^{(l)} := 3\gamma_j + 2l\cdot 2^j$ for $0 \le j \le 2m$, $l \in \{0,1,2\}$. Hence the problem reduces to the computation of

$$\prod_{j=0}^{2m}(1+e^{2\pi i\overline{\gamma}_j^{(l)}/6}) = \prod_{j=0}^{2m} z_j^{(l)},$$

where we set $1+e^{2\pi i\overline{\gamma}_j^{(l)}/6} =: z_j^{(l)} = |z_j^{(l)}|e^{i\phi_j^{(l)}}$. The value of $z_j^{(l)}$ is determined by the residue of $\overline{\gamma}_j^{(l)}$ modulo 6:

$\overline{\gamma}_j^{(l)}$ mod 6	$\lvert z_j^{(l)}\rvert$	$\phi_j^{(l)}$
0	2	0
1	$\sqrt{3}$	$\pi/6$
2	1	$\pi/3$
3	0	0
4	1	$-\pi/3$
5	$\sqrt{3}$	$-\pi/6$

In the following we investigate the residue of $\overline{\gamma}_j^{(l)}$ modulo 6 for the different values of j, l and γ_j. We obtain:

l	j	γ_j	$\overline{\gamma}_j^{(l)}$ mod 6	$\lvert z_j^{(l)}\rvert$	$\phi_j^{(l)}$
0	—	1	3	0	0
0	—	0	0	2	0
1	even	1	5	$\sqrt{3}$	$-\pi/6$
1	odd	1	1	$\sqrt{3}$	$\pi/6$
1	even	0	2	1	$\pi/3$
1	odd	0	4	1	$-\pi/3$
2	even	1	1	$\sqrt{3}$	$\pi/6$
2	odd	1	5	$\sqrt{3}$	$-\pi/6$
2	even	0	4	1	$-\pi/3$
2	odd	0	2	1	$\pi/3$

We have assumed that there is at least one $\gamma_j = 1$, which implies

$$\prod_{j=0}^{2m} z_j^{(0)} = 0.$$

It remains to compute

$$\sum_{\substack{n=0\\ n\equiv 0\,(3)}}^{2^{2m+1}-1} (-1)^{s_{\gamma,2}(n)} = \frac{1}{3}\prod_{j=0}^{2m} z_j^{(1)} + \frac{1}{3}\prod_{j=0}^{2m} z_j^{(2)}.$$

By the table above we have $|z_j^{(1)}| = |z_j^{(2)}|$ and $\phi_j^{(1)} = -\phi_j^{(2)}$ for all possible values of j and γ_j. Therefore we get

$$\begin{aligned}\sum_{\substack{n=0\\ n\equiv 0\,(3)}}^{2^{2m+1}-1} (-1)^{s_{\gamma,2}(n)} &= \frac{1}{3}\Big(\prod_{j=0}^{2m} |z_j^{(1)}|\Big)\big(e^{i\sum_{j=0}^{2m}\phi_j^{(1)}} + e^{-i\sum_{j=0}^{2m}\phi_j^{(1)}}\big)\\ &= \frac{1}{3}\sqrt{3}^{\rho(2m)} 2\cos\Big(\sum_{j=0}^{2m}\phi_j^{(1)}\Big),\end{aligned}$$

where $\rho(2m) := \#\{0 \le j \le 2m \mid \gamma_j = 1\}$. For $\sum_{j=0}^{2m} \phi_j^{(1)}$ we get

$$\begin{aligned}\sum_{j=0}^{2m} \phi_j^{(1)} &= -\frac{\pi}{6}\sum_{j=0}^{2m}\gamma_j(-1)^j + \frac{\pi}{3}\sum_{j=0}^{2m}(1-\gamma_j)(-1)^j \\ &= \frac{\pi}{3}\sum_{j=0}^{2m}(-1)^j - \frac{\pi}{2}\sum_{j=0}^{2m}\gamma_j(-1)^j = \frac{\pi}{3} - \frac{\pi}{2}\sum_{j=0}^{2m}\gamma_j(-1)^j.\end{aligned}$$

So it is easy to check that

$$\frac{2}{3}\cos\Big(\sum_{j=0}^{2m}\phi_j^{(1)}\Big) \in \{\pm 1/\sqrt{3}, \pm 1/3\}$$

and the result follows. ■

3. Discrepancy bounds for NH sequences. From the general proof of the uniform distribution of NH sequences with uniformly distributed components, given in [4], and from the quantitative versions of the results from [7] used in this proof, it is possible to derive discrepancy estimates for NH sequences. However, these estimates, also in the best case, are of the form

$$D_N = O(1/N^{\delta})$$

with some very small $\delta > 0$. So, if we are interested in searching for low-discrepancy sequences, then we have to improve the general result (if possible) by using other techniques or to study the sequences individually in more detail.

We already know that there exist non-trivial (i.e., generated by more than one component) low-discrepancy NH sequences, namely the Halton sequences (which are "finite row" NH sequences).

On the other hand, we know from [6] that there exist NH sequences combined from digital $(0, w_i)$-sequences which definitely are not low-discrepancy sequences, for example the two-dimensional NH sequence generated by the unit matrix in $\mathbb{Z}_3$ and by

$$C := \begin{pmatrix} 1 & 1 & 1 & 1 & \dots \\ 0 & 1 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \in \mathbb{Z}_2^{\mathbb{N}\times\mathbb{N}}$$

(an "infinite row" NH sequence).

We start our analysis with a more general "negative" result on the discrepancy of "infinite row" NH sequences.

THEOREM 2. *Let $(\boldsymbol{x}_n)_{n\geq 0}$ be a NH sequence generated by the unit matrix $C^{(1)}$ in $\mathbb{Z}_3$ and by a matrix $C^{(2)} = (c_{r,j})_{r,j\geq 0}$ in $\mathbb{Z}_2$ which is arbitrary but contains at least one row with positive upper density d of ones, i.e.,*

$$\limsup_{k\to\infty} \frac{1}{k}\,\#\{0 \leq j \leq k-1 \mid c_{r,j} = 1\} = d > 0$$

for at least one r. Then for the discrepancy D_N^* of this sequence we have

$$ND_N^* = \Omega(N^\delta)$$

for every $\delta < d\cdot\log 3/\log 4$ (i.e., $ND_N^* \geq cN^\delta$ for a fixed constant $c > 0$ and infinitely many N).

Proof. For $\epsilon > 0$ let $k = 2m+1$ be such that

$$\#\{0 \leq j \leq k-1 \mid c_{r,j} = 1\} =: e > (d-\epsilon)k.$$

There are infinitely many such k. We consider the set

$$J := [0,1/3) \times \bigcup_{a=0}^{2^{r-1}-1} \left[\frac{a}{2^{r-1}}, \frac{a}{2^{r-1}} + \frac{1}{2^r}\right)$$

and $N = 2^k$. Let the indices $j_1 < \cdots < j_e$ be such that $c_{r,j_i} = 1$. Then $\boldsymbol{x}_n \in J$ for $0 \leq n < 2^k$ if and only if $n \equiv 0\ (3)$ and $n_{j_1} + \cdots + n_{j_e} \equiv 0\ (2)$. Hence

$$\begin{aligned}&|\#\{0 \leq n < N \mid \boldsymbol{x}_n \in J\} - N\cdot\lambda(J)|\\ &\qquad = |\#\{0 \leq n < N \mid n \equiv 0\ (3) \text{ and } s_{\gamma,2}(n) \equiv 0\ (2)\} - N/6|,\end{aligned}$$

where $\gamma = (\gamma_0, \ldots, \gamma_{2m})$ with $\gamma_j = 1$ iff $j = j_i$ for $i = 1, \ldots, e$. By Theorem 1 the above difference is at least $\geq \frac{1}{3}3^{e/2}$. Therefore for at least one $a \in \{0, 1, \ldots, 2^{r-1}-1\}$ and for $J_a := [0,1/3) \times [a/2^{r-1}, a/2^{r-1} + 1/2^r)$ we have

$$\begin{aligned}|\#\{0 \leq n < N \mid \boldsymbol{x}_n \in J_a\} - N\cdot\lambda(J_a)| &\geq \frac{1}{2^{r-1}}\,\frac{1}{3}\,3^{e/2}\\ &> cN^{(d-\epsilon)\log 3/\log 4},\end{aligned}$$

and the result follows. ∎

This result does not give much hope to find large classes of low-discrepancy point sequences within the class of "infinite row" NH sequences, and it seems reasonable to study "finite row" NH sequences. A first step in this direction was already done in [6] where a general upper bound for the discrepancy of "finite row" NH sequences was provided. This is a rather technical bound which was not discussed further in [6]. For our purposes it suffices to give a slightly simplified form of this bound.

Let $C_1, \ldots, C_s$ be the generating matrices of a "finite row" NH sequence. For arbitrary non-negative integers $d_1, \ldots, d_s$ let $L(d_1, \ldots, d_s)$ be minimal such that for all $i \in \{1, \ldots, s\}$ each of the first d_i rows of C_i has length less than or equal to $L(d_1, \dots, d_s)$. By the *length* of the row $(c_{j,1}\, c_{j,2}\, c_{j,3} \dots)$ we mean $\max\{k \geq 1 \mid c_{j,k} \neq 0\}$, respectively 0 for the zero row. With the help of this length parameter L we can formulate the discrepancy estimate for “finite row” NH sequences given in [6, Theorem 3.1].

Let $(\boldsymbol{x}_n)_{n\geq 0}$ be a “finite row” NH sequence formed by uniformly distributed digital $(\mathbf{T}_i, w_i)$-sequences in base q_i. Then for the discrepancy of this sequence we have

$$D_N \leq \frac{2c}{N} \sum_{\substack{\boldsymbol{k} \\ Q(\boldsymbol{k}) \leq N}} Q(\boldsymbol{k}) P(\boldsymbol{k}) + R, \tag{1}$$

where

$$\begin{aligned} \boldsymbol{k} &= (k_{1,1}, \dots, k_{1,w_1}, k_{2,1}, \dots, k_{2,w_2}, \dots, k_{v,1}, \dots, k_{v,w_v}) \in \mathbb{N}_0^s, \\ P(\boldsymbol{k}) &:= \prod_{i=1}^{v} \prod_{j=1}^{w_i} q_i^{-k_{i,j}}, \qquad Q(\boldsymbol{k}) := \prod_{i=1}^{v} q_i^{L(k_{i,1}, \dots, k_{i,w_i})}, \\ c &= \prod_{i=1}^{v} q_i^{w_i}, \end{aligned}$$

and R is a positive remainder term which will be needed only in the proof of Theorem 3 and hence will be dealt with there.

Remark 1. In searching for low-discrepancy point sequences the estimate (1) can only help when all generating digital $(\mathbf{T}_i, w_i)$-sequences are of dimension 1, i.e., $w_i = 1$ for all i. This is because we will show that for a NH sequence with $v \geq 2$ and $w_i \geq 2$ for at least one i, for the right hand side (RHS) of (1) we always have

$$\text{RHS} \geq c' \frac{1}{\sqrt{N}}$$

for infinitely many N with a positive constant c'.

Proof. We may only show this for $v = 2$, $w_1 = 2, w_2 = 1$ since $(\boldsymbol{x}_n)_{n\geq 0}$ contains at least one such three-dimensional projection. We can assume that the projection of $(\boldsymbol{x}_n)_{n\geq 0}$ to the first two coordinates corresponding to w_1 is a digital $(\mathbf{T}, 2)$-sequence with $\lim_{m\to\infty}(m - \mathbf{T}(m)) = +\infty$. Otherwise the projection and consequently $(\boldsymbol{x}_n)_{n\geq 0}$ itself would not be uniformly distributed.

So there are sequences $u_1 < u_2 < \cdots$ and $m_1 < m_2 < \cdots$ of positive integers with $m_i - \mathbf{T}(m_i) = u_i$. Let $d_1, d_2 \geq 0$ be arbitrary integers such that $d_1 + d_2 = u_i$. Then the first d_1 rows of $C^{(1)}$ and the first d_2 rows of $C^{(2)}$ ($C^{(1)}$ and $C^{(2)}$ are the generator matrices of the digital sequence) are together linearly independent and therefore $L(d_1, d_2) \geq u_i$.

In particular, $L(\lceil u_i/2\rceil, 0) \geq u_i$ or $L(0, \lceil u_i/2\rceil) \geq u_i$, say the former. Then for all (infinitely many) $N = q_1^{L(\lceil u_i/2\rceil,0)}$ we have

$$\text{RHS} \geq \frac{2c}{N} \sum_{\substack{\boldsymbol{k} \\ \boldsymbol{k}=(\lceil u_i/2\rceil,0,0)}} Q(\boldsymbol{k})P(\boldsymbol{k}) = \frac{2c}{q_1^{L(\lceil u_i/2\rceil,0)}}\, q_1^{L(\lceil u_i/2\rceil,0)} q_1^{-\lceil u_i/2\rceil}$$

$$= \frac{2c}{q_1^{\lceil u_i/2\rceil}} \geq \frac{2c}{q_1^{(L(\lceil u_i/2\rceil,0)+1)/2}} = \frac{2c}{\sqrt{q_1}} \cdot \frac{1}{\sqrt{N}}. \ \blacksquare$$

For the case of $w_i = 1$ for all i, to obtain a uniformly distributed NH sequence we trivially must have

$$L^{(i)}(d) := L(\underbrace{0, \ldots, 0, d}_{i}, 0, \ldots, 0) \geq d$$

for all i and d.

The discrepancy bound in (1) will give us useful (low-discrepancy) results for the case that $L^{(i)}(d) \leq d + v$ for all i and d and a fixed constant v. (For example for the Halton sequence we have $v = 0$ and for the Halton sequence based on Gray Code digits (see [5] or [3]) we have $v = 1$.)

THEOREM 3. *Let $(\boldsymbol{x}_n)_{n\geq 0}$ be a NH sequence with $w_i = 1$ for all i and $L^{(i)}(d) \leq d+v$ for all i and d, with fixed constant v. Then for the discrepancy D_N^* of $(\boldsymbol{x}_n)_{n\geq 0}$, for all N large enough we have*

$$D_N^* \leq c'(q_1 \cdots q_s)^{2v} (\log N)^s / N$$

with c' depending only on $s, q_1, \ldots, q_s$.

Proof. If $w_i = 1$ for all i and $L^{(i)}(d) \leq d + v$ for all i and d it can easily be seen by checking the rather technical definition of the remainder term R of the RHS in (1) given in [6], that R can be absorbed by the first term of RHS, i.e.,

$$(2) \qquad D_N^*(\omega) \leq c''(q_1 \cdots q_s)^v \frac{1}{N} \sum_{\substack{\boldsymbol{k} \\ Q(\boldsymbol{k}) \leq N}} Q(\boldsymbol{k})P(\boldsymbol{k})$$

with a certain constant c'' depending only on $s, q_1, \ldots, q_s$. (We will not go into the technical details of this fact here, but for the reader who will undertake this task we just note that in this special case

$$L(\tilde{\zeta}(i_0, j_0, \theta + 1)) \leq L(\tilde{\zeta}(i_0, j_0, \theta)) + v + 1,$$
$$Q(\tilde{\zeta}(i_0, j_0, \theta + 1)) \leq Q(\tilde{\zeta}(i_0, j_0, \theta)) \cdot q_{i_0}^{v+1},$$

and since by definition of θ,

$$Q(\tilde{\zeta}(i_0, j_0, \theta)) \leq N \leq Q(\tilde{\zeta}(i_0, j_0, \theta + 1)),$$

we have $N/Q(\tilde{\zeta}(i_0, j_0, \theta)) \leq q_{i_0}^{v+1}$.) Now the result immediately follows by inserting in (2). ■

But already if $L^{(i)}(d)$ grows slightly faster than d, for example if $L^{(i)}(d) = d(1+\epsilon)$ for infinitely many d, then the RHS of (1) is not helpful any more.

Remark 2. For example, if $(\boldsymbol{x}_n)_{n\geq 0}$ is a NH sequence with $w_i = 1$ for all i, $L^{(1)}(d) = d(1+\epsilon)$ for all d and $L^{(i)}(d) = d$ for all $i \geq 2$ and all d, then for the RHS of (1) we get

$$\begin{aligned}\text{RHS} &\geq \frac{2c}{N} \sum_{\substack{k_1,k_2,\ldots,k_s \\ q_1^{k_1(1+\epsilon)} q_2^{k_2} \cdots q_s^{k_s} \leq N}} q_1^{\epsilon k_1} \geq \frac{2c}{N} \sum_{\substack{k_1 \\ q_1^{k_1(1+\epsilon)} \leq N}} q_1^{\epsilon k_1} \\ &\geq c' \frac{1}{N^{1/(1+\epsilon)}}\end{aligned}$$

(with $c' > 0$ depending only on $s, q_1, \ldots, q_s$).

The RHS of (1) shows a strong dependence on the length of the rows of the generator matrices, which is quite astonishing. So of course we have to ask if the discrepancy bound (1) is too weak, and whether it could be improved so as to get rid of the essential dependence on L in this bound. However, we will show by examples that this is not possible in general, and that the dependence of the discrepancy of a NH sequence on the parameter L is essential.

Example 1. Let $(\boldsymbol{x}_n)_{n\geq 0}$ be a NH sequence generated by the unit matrix in $\mathbb{Z}_3$ and a matrix $C^{(2)} = (c_{i,j}^{(2)})_{i,j\geq 1}$ in $\mathbb{Z}_2$ with finite rows of the following form.

Assume there are row indices $r_1 < r_2 < \cdots$, a $\rho > \log 4/\log 3$, an $\epsilon > 0$ and for each r_i an odd k_i such that

$$e_i := \#\{1 \leq j \leq k_i \mid c_{r_i,j}^{(2)} = 1\} > \max\{\rho r_i, \epsilon k_i\}.$$

That means: there are infinitely many rows in which the number of 1s is "not too small" ($> \rho r_i$) and "not too thin" ($> \epsilon k_i$).

A concrete example is given by $C^{(2)}$ with

$$c_{i,j}^{(2)} = \begin{cases} 1 & \text{for } i \leq j \leq (1+\kappa)i, \\ 0 & \text{otherwise,} \end{cases}$$

with some $\kappa > \log 4/\log 3$.

We show that for the discrepancy of such sequences we have

$$ND_N^* \geq N^\delta$$

for infinitely many N and

$$\delta := \left(1 - \frac{1}{\rho}\frac{\log 4}{\log 3}\right) \cdot \epsilon > 0.$$

Proof. Consider $N = 2^{k_i}$ (note that $k_i \geq r_i$) and the set

$$J := [0, 1/3) \times \bigcup_{a=0}^{2^{r_i-1}-1} \left[\frac{a}{2^{r_i-1}}, \frac{a}{2^{r_i-1}} + \frac{1}{2^{r_i}}\right) =: \bigcup_{a=0}^{2^{r_i-1}-1} J_a,$$

a union of 2^{r_i-1} intervals of total volume $1/(3 \cdot 2^{r_i})$.

Let $j_1 < \cdots < j_{e_i} \leq k_i$ be such that $c_{r_i, j_l} = 1$. Then $\boldsymbol{x}_n \in J$ if and only if $n \equiv 0\ (3)$ and $n_{j_1} + \cdots + n_{j_{e_i}} \equiv 0\,(2)$.

By Theorem 1 we have

$$|\#\{0 \leq n < N \mid n \equiv 0\ (3) \text{ and } n_{j_1} + \cdots + n_{j_{e_i}} \equiv 0\ (2)\} - N/6| > \frac{1}{3}\, 3^{e_i/2}.$$

Hence for at least one a we have

$$\left|\#\{0 \leq n < N \mid \boldsymbol{x}_n \in J_a\} - \frac{N}{3 \cdot 2^{r_i}}\right| > \frac{2}{3}\,\frac{1}{2^{r_i}}\, 3^{e_i/2} > \left(\frac{3^{1/2}}{2^{1/\rho}}\right)^{\epsilon \cdot k_i} = N^{\delta}. \blacksquare$$

It is plausible that the discrepancy does not depend on the *length* of the rows of the generator matrices but on the *number of* 1*s* in the rows. Until now, we have not been able to decide this question. The above results leave the following problems open.

Open Problem 1. *Determine whether the following two-dimensional NH sequences in bases* 3 *and respectively* 2 *are low-discrepancy sequences or not (respectively: give good lower and upper bounds for their discrepancy):*

1. $C^{(1)}$ *the unit matrix in* $\mathbb{Z}_3$ *and*

$$C^{(2)} = \begin{pmatrix} 1 & \underbrace{00\ldots0}_{l_1} & 1 & 0 & 0 & \ldots & & & \\ 0 & 1 & \underbrace{00\ldots\ldots0}_{l_2} & 1 & 0 & 0 & \ldots & & \\ 0 & 0 & 1 & \underbrace{00\ldots\ldots\ldots0}_{l_3} & 1 & 0 & 0 & \ldots & \\ \vdots & \vdots & \vdots & \ddots & \vdots & & & & \end{pmatrix}$$

in $\mathbb{Z}_2$ *with* $l_1, l_2, l_3, \ldots$ *arbitrary but* $\limsup_{i\to\infty} l_i = +\infty$.

2. $C^{(1)}$ *the unit matrix in* $\mathbb{Z}_3$ *and*

$$C^{(2)} = \begin{pmatrix} 1 & \overbrace{00\ldots0}^{l_1} & 1 & \overbrace{00\ldots0}^{l_2} & 1 & 0 & \ldots \\ 0 & 1 & 0 & 0 & 0 & 0 & \ldots \\ 0 & 0 & 1 & 0 & 0 & 0 & \ldots \\ \vdots & \vdots & \vdots & \ddots & \vdots & & \end{pmatrix} \in \mathbb{Z}_2^{\mathbb{N}\times\mathbb{N}}.$$

The first row contains infinitely many 1*s but with density* 0. *(*$l_1, l_2, \ldots$ *can be chosen such that the* 1*s are arbitrarily thin in the first row).*

3.

$$C^{(1)} = C^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 1 & \dots \\ 0 & 1 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

but $C^{(1)}$ in $\mathbb{Z}_3$ and $C^{(2)}$ in $\mathbb{Z}_2$. We conjecture that $ND^*_N = \Omega(N^\delta)$ for some $\delta > 0$. A proof would need lower bounds for the results of Kim in [7] *on the joint distributions of sums of digits in different bases.*

Even if it is possible to give sharper discrepancy estimates for "finite row" NH sequences which are applicable also for the general case of $w_i \geq 2$ for some i, we would still have the following problem. Until now, we do not know any digital (t, s)-sequence in dimension $s \geq 2$ which is generated by matrices with finite rows exclusively.

All low-discrepancy digital (t, s)-sequences in dimension $s \geq 2$ provided until now by Sobol' [12], Faure [2], Niederreiter [11], Niederreiter–Xing [13], et al. have been generated by matrices with infinite rows also.

So until now we also do not know if there exist low-discrepancy "finite row" NH sequences with $w_i \geq 2$ for some i. This gap will be filled in the next section by proving for arbitrary dimension s the existence of digital $(0, s)$-sequences generated by matrices with finite rows of—in some sense—shortest possible length. We will also give concrete examples.

4. Digital $(0, s)$-sequences generated by matrices with finite rows.

Since we have claimed to provide in some sense shortest possible row lengths, we first give a lower bound for the row lengths.

Proposition 1. *Let $C_1, \dots, C_s$ be the generator matrices of a digital $(0, s)$-sequence in prime base $q \geq s$. Then for every positive integer d there exists $i \in \{1, \dots, s\}$ such that*

$$L(\underbrace{0, \dots, 0}_{i-1}, d, 0, \dots, 0) \geq sd.$$

Proof. Assume that there is a $d > 0$ such that for all $i \in \{1, \dots, s\}$,

$$L(\underbrace{0, \dots, 0}_{i-1}, d, 0, \dots, 0) < sd.$$

We consider the $sd \times sd$-matrix consisting of

the upper left $d \times sd$-submatrix of C_1 together with
the upper left $d \times sd$-submatrix of C_2 together with
$\vdots$
the upper left $d \times sd$-submatrix of C_s.

This matrix does not have rank sd, since the last column is a zero column. This contradicts $\mathbf{T} \equiv 0$. ■

If we assume that for a digital $(0,s)$-sequence in prime base $q \geq s$ we have $L(d,0,\dots,0) = sd$ for all $d \in \mathbb{N}$, we can deduce by a similar argument that for all $d \in \mathbb{N}$ there exists $i \in \{2,\dots,s\}$ such that

$$L(\underbrace{0,\dots,0}_{i-1},d,0,\dots,0) \geq sd-1.$$

In the next step we assume that $L(d,0,\dots,0) = sd$ and $L(0,d,0,\dots,0) = sd-1$ for all $d \in \mathbb{N}$ and deduce that for all $d \in \mathbb{N}$ there exists $i \in \{3,\dots,s\}$ such that $L(\underbrace{0,\dots,0}_{i-1},d,0,\dots,0) \geq sd-2$ and so on.

Step by step we get a certain lower bound for the parameter L.

In the following we search for in a certain sense "optimal" digital $(0,s)$-sequences in prime base $q \geq s$ with generator matrices $C_1,\dots,C_s$ such that for every $i \in \{1,\dots,s\}$ we have

$$L(\underbrace{0,\dots,0}_{i-1},d,0,\dots,0) = sd-(i-1)$$

for all $d \in \mathbb{N}$. We call such digital $(0,s)$-sequences *generated by matrices with lowest possible row lengths*.

4.1. On existence of digital $(0,s)$-sequences generated by matrices with lowest possible row lengths. In order to ensure that there exist digital $(0,s)$-sequences generated by matrices with lowest possible row lengths, we modify digital $(0,s)$-sequences in prime base $q \geq s$. The latter sequences exist: examples were introduced by Faure [2] and also by Sobol' [12] for $q=2$ based on the Pascal matrices given in the following example.

EXAMPLE 2. The *Pascal matrices* $P^{(0)},P^{(1)},\dots,P^{(q-1)}$ in prime base q are defined by

$$P^{(i)} := \begin{pmatrix} 1 & \binom{1}{0}i^1 & \binom{2}{0}i^2 & \binom{3}{0}i^3 & \dots \\ 0 & 1 & \binom{2}{1}i^1 & \binom{3}{1}i^2 & \dots \\ 0 & 0 & 1 & \binom{2}{1}i^1 & \dots \\ \vdots & \vdots & \vdots & \ddots & \vdots \end{pmatrix} \in \mathbb{Z}_q^{\mathbb{N}\times\mathbb{N}}$$

modulo q, where $i \in \{0,1,\dots,q-1\}$. It is well known that the matrices $P^{(0)},P^{(1)},\dots,P^{(q-1)}$ generate a digital $(0,q)$-sequence in base q. Note that each Pascal matrix is a non-singular upper triangular matrix (NUT matrix) and $P^{(0)}$ is the unit matrix in $\mathbb{Z}_q$.

The following theorem yields existence of a digital $(0,s)$-sequence in prime base $q \geq s$ generated by matrices consisting of rows with lowest possible lengths.

Theorem 4. *For all $s \geq 1$ and all primes $q \geq s$ there exist matrices $C'_1, \dots, C'_s \in \mathbb{Z}_q^{\mathbb{N}\times\mathbb{N}}$ that are generator matrices with lowest possible row lengths of a $(0,s)$-sequence in base q.*

We prove the existence of such matrices by scrambling the digital $(0,s)$-sequence in prime base $q \geq s$. Thereby we also provide a construction principle for such sequences.

Our method of scrambling is based on the following result of Faure and Tezuka [3, Proposition 1]:

Lemma 1. *Let $C_1, \dots, C_s \in \mathbb{Z}_q^{\mathbb{N}\times\mathbb{N}}$ be the generator matrices of a digital $(0,s)$-sequence in prime base $q \geq s$. If M is a NUT matrix in $\mathbb{Z}_q$, then the matrices $C_1M, \dots, C_sM$ generate a digital $(0,s)$-sequence in prime base $q \geq s$.*

Proof of Theorem 4. Let $q \in \mathbb{P}$ and $s \leq q$ be fixed. We choose matrices $C_1, \dots, C_s \in \mathbb{Z}_q^{\mathbb{N}\times\mathbb{N}}$ which generate a digital $(0,s)$-sequence in prime base $q \geq s$. Such matrices exist by Example 2. In the following we search for a scrambling NUT matrix M such that $C'_1 := C_1M, \dots, C'_s := C_sM$ are generator matrices with lowest possible row lengths of a digital $(0,s)$-sequence in prime base $q \geq s$. Hence

$$\begin{aligned} L(d,0,0,\dots,0,0) &= sd \quad \forall d \in \mathbb{N},\\ L(0,d,0,\dots,0,0) &= sd-1 \quad \forall d \in \mathbb{N},\\ &\vdots\\ L(0,0,0,\dots,0,d) &= sd-(s-1) \quad \forall d \in \mathbb{N}. \end{aligned}$$

By the structure of the problem we can determine the matrix M columnwise.

Fix $m \in \mathbb{N}$. In the following we determine the mth column of M, denoted by c_m. Since M is an UT matrix, we just have to determine the first m entries of c_m (all others are 0). Since M is non-singular as well, we set the mth entry of c_m equal to 1. Thus all diagonal entries of M are 1. In order to determine the remaining $m-1$ unknown entries of c_m we consider the desired parameter L of the above form.

- The dth row of $C'_1 = C_1M$ should have length $(\leq)$ ds for all $d \in \mathbb{N}$. This is guaranteed if at least the first $\lfloor (m-1)/s \rfloor$-entries of the mth column of C'_1 are zero. (Here and later on $\lfloor x \rfloor$ denotes the integer part of a real x.)

- Analogously, we set the first $\lfloor m/s \rfloor$-entries of the mth column of C_2' equal to zero to guarantee that the dth row of C_2' has length $(\leq)$ $ds-1$ for all $d \in \mathbb{N}$.

$\vdots$

- Finally, we set the first $\lfloor (m+s-2)/s \rfloor$-entries of the mth column of C_s' equal to zero to guarantee that the dth row of C_s' has length $(\leq)$ $ds-(s-1)$ for all $d \in \mathbb{N}$.

Altogether, we get $m-1$ fixed zero entries in the mth columns of $C_1', \dots, C_s'$, since

$$\sum_{i=1}^{s} \left\lfloor \frac{m+i-2}{s} \right\rfloor = m-1.$$

This can be easily checked by setting $m = qs + r$ where $q \in \mathbb{N}_0$ and $r \in \{0, 1, \dots, s-1\}$.

Hence the first $m-1$ unknown entries of the mth column of M can be determined from the following system of equations:

$$D \cdot (c_{1,m}, c_{2,m}, \dots, c_{m-1,m}, 1, 0, 0, \dots)^\top = (\underbrace{0, 0, \dots, 0}_{m-1})^\top,$$

where D is the matrix $\in \mathbb{Z}_q^{(m-1)\times\mathbb{N}}$ formed by

the first $\lfloor (m-1)/s \rfloor$ rows of C_1 together with
the first $\lfloor m/s \rfloor$ rows of C_2 together with
$\vdots$
the first $\lfloor (m+s-2)/s \rfloor$ rows of C_s.

Since $C_1, \dots, C_s$ are generator matrices of a digital $(0, s)$-sequence in prime base $q \geq s$, the left $(m-1) \times (m-1)$-submatrix of D has full rank. Hence the $m-1$ unknown entries of c_m, namely $c_{1,m}, c_{2,m}, \dots, c_{m-1,m}$, are uniquely determined.

Since m was arbitrarily chosen, the matrix M with the properties claimed above can be determined columnwise and the matrices $C_1', \dots, C_s'$ with "lowest possible parameter L" can be computed by matrix multiplication. ∎

The proof above already provides an algorithm to obtain matrices $C_1', \dots, C_s'$ consisting of rows of lowest possible lengths which generate a $(0, s)$-sequence.

In the next subsection we give explicit examples. We investigate digital $(0, s)$-sequences in prime base $q \geq s$ generated by s Pascal matrices in base q for $s = 1$, $s = 2$ and $s = q$. The aim is to determine scrambling matrices which lead to digital $(0, s)$-sequences in prime base $q \geq s$ generated by matrices with lowest possible row lengths. Furthermore, we discover some interesting properties of these scrambling matrices and the generator matrices with lowest possible row lengths.

4.2. Concrete examples. In the previous subsection we proved existence of digital $(0,s)$-sequences in any prime base $q \geq s$ such that the generator matrices have best possible L parameter and we provided a general construction principle. In this subsection, we give explicit examples by applying the above method to Pascal matrices.

We redefine the ith Pascal matrix in base q by $P^{(i)} := (p_{j,k}^{(i)})_{j,k\geq 1}$. The kth entry of the jth row in $P^{(i)}$ is given by

$$p_{j,k}^{(i)} = \begin{cases} \binom{k-1}{j-1} i^{k-j}, & 1 \leq j \leq k, \\ 0, & j > k, \\ 0, & j \leq 0, \end{cases}$$

modulo q, where $k \in \mathbb{N}$, $j \in \mathbb{Z}$ and $0^0 := 1$. Here we extend the domain of j, because this will be useful for the investigations in this subsection. In the following, $P^{(i)}$ will sometimes be denoted by $P^{(i)} = (\mathrm{col}_1^{(i)}, \mathrm{col}_2^{(i)}, \mathrm{col}_3^{(i)}, \ldots)$, where $\mathrm{col}_k^{(i)}$ is the kth column of $P^{(i)}$.

Proposition 2. *Let $q \in \mathbb{P}$. The set $P^{(0)}, P^{(1)}, \ldots, P^{(q-1)}$ with matrix multiplication $\circ$ forms an abelian group with $P^{(i)} \circ P^{(j)} = P^{(i+j\,(q))}$ for all $i, j \in \mathbb{Z}_q$.*

Proof. It suffices to prove $P^{(i)} \circ P^{(j)} = P^{(i+j\,(q))}$ for all $i, j \in \mathbb{Z}_q$.

We define $C := P^{(i)} \circ P^{(j)}$, compute $c_{m,n}$ and compare it to $p_{m,n}^{(i+j)}$. Since all $P^{(k)}$ are NUT matrices it suffices to check the case $m \leq n$ (otherwise we get the trivial equation $0 = 0$):

$$c_{m,n} = \sum_{l=1}^{\infty} p_{m,l}^{(i)} p_{l,n}^{(j)} = \sum_{l=m}^{n} \binom{l-1}{m-1} i^{l-m} \binom{n-1}{l-1} j^{n-l},$$

$$\begin{aligned} p_{m,n}^{(i+j)} &= \binom{n-1}{m-1}(i+j)^{n-m} = \sum_{l=0}^{n-m} \binom{n-1}{m-1}\binom{n-m}{l} i^l j^{n-m-l} \\ &= \sum_{l=m}^{n} \binom{n-1}{m-1}\binom{n-m}{l-m} i^{l-m} j^{n-l}. \end{aligned}$$

It is easy to check the equality of $\binom{n-1}{m-1}\binom{n-m}{l-m}$ and $\binom{l-1}{m-1}\binom{n-1}{l-1}$, which concludes the proof. ■

For each $i \in \{0, \ldots, q-1\}$ we can scramble the $(0,1)$-sequence generated by $P^{(i)}$ using its inverse $P^{(q-i)}$ as scrambling matrix. Hence the resulting matrix fulfills $L(d) = d$ for all $d \in \mathbb{N}$. Columnwise construction, as in the proof of Theorem 4, would provide the same scrambling matrix.

In the next theorem we define for each $i \in \{1, \ldots, q-1\}$ a NUT matrix $M \in \mathbb{Z}_q^{\mathbb{N}\times\mathbb{N}}$ such that the matrices $M = P^{(0)}M$ and $P^{(i)}M$ satisfy $L(d,0) = 2d$ and $L(0,d) = 2d-1$ for all $d \in \mathbb{N}$.

THEOREM 5. *Let $i \in \{1, \dots, q-1\}$. The matrix $M \in \mathbb{Z}_q^{\mathbb{N}\times\mathbb{N}}$ defined by*

$$M := \begin{pmatrix} \mathrm{col}_1^{(q-i)} & \mathrm{col}_2^{(q-i)} & \begin{pmatrix} 0 \\ \mathrm{col}_2^{(q-i)} \end{pmatrix} & \begin{pmatrix} 0 \\ \mathrm{col}_3^{(q-i)} \end{pmatrix} & \begin{pmatrix} 0 \\ 0 \\ \mathrm{col}_3^{(q-i)} \end{pmatrix} & \cdots \end{pmatrix}$$

and the matrix $P^{(i)}M \in \mathbb{Z}_q^{\mathbb{N}\times\mathbb{N}}$ generate a digital $(0,2)$-sequence in prime base q and satisfy $L(d,0) = 2d$ and $L(0,d) = 2d-1$ for all $d \in \mathbb{N}$. Furthermore,

$$P^{(i)}M = \begin{pmatrix} 1 & 0 & 0 & \dots \\ 0 & & & \\ 0 & & \overline{M} & \\ \vdots & & & \end{pmatrix},$$

where

$$\overline{M} = \begin{pmatrix} \mathrm{col}_1^{(i)} & \mathrm{col}_2^{(i)} & \begin{pmatrix} 0 \\ \mathrm{col}_2^{(i)} \end{pmatrix} & \begin{pmatrix} 0 \\ \mathrm{col}_3^{(i)} \end{pmatrix} & \begin{pmatrix} 0 \\ 0 \\ \mathrm{col}_3^{(i)} \end{pmatrix} & \begin{pmatrix} 0 \\ 0 \\ \mathrm{col}_4^{(i)} \end{pmatrix} & \dots \end{pmatrix}.$$

EXAMPLE 3. In the special case of $s = q = 2$ the following matrices with lowest possible row lengths generate a digital $(0,2)$-sequence in base 2:

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & \dots \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \dots \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & \dots \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Theorem 5 can be derived from the following proposition.

PROPOSITION 3. *For all $i \in \{1, \dots, q-1\}$ and all $m \in \mathbb{N}$,*

$$P^{(i)} \begin{pmatrix} \left.\begin{matrix} 0 \\ \vdots \\ 0 \end{matrix}\right\} m-1 \\ \mathrm{col}_m^{(q-i)} \end{pmatrix} = \begin{pmatrix} \left.\begin{matrix} 0 \\ \vdots \\ 0 \end{matrix}\right\} m-1 \\ \mathrm{col}_m^{(i)} \end{pmatrix} \in \mathbb{Z}_q^{\mathbb{N}} \tag{3}$$

and

$$P^{(i)} \begin{pmatrix} \left.\begin{matrix} 0 \\ \vdots \\ 0 \end{matrix}\right\} m-1 \\ \mathrm{col}_{m+1}^{(q-i)} \end{pmatrix} = \begin{pmatrix} \left.\begin{matrix} 0 \\ \vdots \\ 0 \end{matrix}\right\} m \\ \mathrm{col}_m^{(i)} \end{pmatrix} \in \mathbb{Z}_q^{\mathbb{N}}. \tag{4}$$

Proof of Theorem 5. Proposition 3 implies

$$P^{(i)}M = \begin{pmatrix} 1 & 0 & 0 & \dots \\ 0 & & & \\ 0 & & \overline{M} & \\ \vdots & & & \end{pmatrix}.$$

Note that the first entry of $\mathrm{col}_1^{(i)}$ is 1 for all $i \in \{0,1,\dots,q-1\}$, since $p_{1,1}^{(i)} = \binom{0}{0} i^0 = 1$. If M is used as scrambling matrix (note that by the definition of M it is an UT matrix and its diagonal entries are all non-zero, hence it is a NUT matrix), we get a pair of matrices $M = P^{(0)}M$ and $P^{(i)}M$ in $\mathbb{Z}_q$ which generate a $(0,2)$-sequence in prime base q with $L(d,0) = 2d$ and $L(0,d) = 2d-1$ for all $d \in \mathbb{N}$. ∎

For the proof of Proposition 3 we need the following lemma, which is easy to check.

Lemma 2. *Let $i \in \{0,\dots,q-1\}$. Then*

$$p_{j+1,k+1}^{(i)} = ip_{j+1,k}^{(i)} + p_{j,k}^{(i)} \quad \textit{for all } k \in \mathbb{N}, j \in \mathbb{Z}. \tag{5}$$

Proof of Proposition 3. The proof is by induction.

Proof of (3).

$m = 1$: Since $P^{(q-i)}$ is inverse to $P^{(i)}$ (see Proposition 2) and $\mathrm{col}_1^{(i)}$ is equal to the first column in I, this holds trivially.

$m \to m+1$: It is easy to check that (3) holds for any fixed $m \in \mathbb{N}$ if and only if

$$\sum_{j=1}^{\infty} p_{r,j}^{(i)} p_{j-m+1,m}^{(q-i)} \equiv p_{r-m+1,m}^{(i)} \ (q) \tag{6}$$

for all $r \in \mathbb{N}$. (Note that (6) is trivially fulfilled for all integers $r \le 0$.) We assume that (6) holds (for all $r \in \mathbb{N}$) for all natural $1,\dots,m$ and prove (6) for $m+1$. Fix $r \in \mathbb{N}$. By Lemma 2 we have

$$(*) := \sum_{j=1}^{\infty} p_{r,j}^{(i)} p_{j-m,m+1}^{(q-i)} = \sum_{j=1}^{\infty} p_{r,j}^{(i)} p_{j-m,m}^{(q-i)}(q-i) + \sum_{j=1}^{\infty} p_{r,j}^{(i)} p_{j-m-1,m}^{(q-i)}.$$

An index shift together with the fact that $p_{j,k}^{(q-i)} = 0$ for $j \le 0$ yields

$$(*) = \sum_{j=1}^{\infty} (p_{r,j+1}^{(i)}(q-i) + p_{r,j+2}^{(i)}) p_{j-m+1,m}^{(q-i)}.$$

Twofold application of Lemma 2 leads to

$$p_{r,j+1}^{(i)}(q-i) + p_{r,j+2}^{(i)} = p_{r,j+1}^{(i)}(q-i) + p_{r,j+1}^{(i)} i + p_{r-1,j+1}^{(i)} \equiv p_{r-1,j}^{(i)} i + p_{r-2,j}^{(i)} \ (q)$$

and we get

$$(*) \equiv \sum_{j=1}^{\infty} (p_{r-1,j}^{(i)} i + p_{r-2,j}^{(i)}) p_{j-m+1,m} \ (q).$$

By the induction hypothesis we obtain

$$(*) \equiv p_{r-m,m}^{(i)} i + p_{r-m-1,m}^{(i)} \ (q).$$

Application of Lemma 2 one more time leads to the desired result

$$\sum_{j=1}^{\infty} p_{r,j}^{(i)} p_{j-m,m+1}^{(q-i)} \equiv p_{r-m,m+1}^{(i)} \ (q).$$

Proof of (4).

$m = 1$: Since $P^{(q-i)}$ is inverse to $P^{(i)}$ it follows that $P^{(i)}\mathrm{col}_2^{(q-i)}$ is the second column of the unit matrix I, which is equal to $(0, \mathrm{col}_1^{(i)})^\top$.

We multiply (4) with $P^{(q-i)}$ and obtain an equivalent version:

$$P^{(q-i)} \begin{pmatrix} \left.\begin{matrix} 0 \\ \vdots \\ 0 \end{matrix}\right\} m \\ \mathrm{col}_m^{(i)} \end{pmatrix} = \begin{pmatrix} \left.\begin{matrix} 0 \\ \vdots \\ 0 \end{matrix}\right\} m-1 \\ \mathrm{col}_{m+1}^{(q-i)} \end{pmatrix} \in \mathbb{Z}_q^{\mathbb{N}}.$$

$m \to m+1$: It is easy to check that (4) holds for a fixed $m \in \mathbb{N}$ if and only if

$$\sum_{j=1}^{\infty} p_{r,j}^{(q-i)} p_{j-m,m}^{(i)} \equiv p_{r-m+1,m+1}^{(q-i)} \ (q) \tag{7}$$

for all $r \in \mathbb{N}$. (Note that (7) is trivially fulfilled for all integers $r \leq 0$.) We assume that (7) holds (for all $r \in \mathbb{N}$) for all natural $1, \ldots, m$ and consider (7) for $m+1$. Let $r \in \mathbb{N}$ and

$$\sum_{j=1}^{\infty} p_{r,j}^{(q-i)} p_{j-m-1,m+1}^{(i)} =: (**).$$

By Lemma 2 we get

$$(**) = \sum_{j=1}^{\infty} i p_{r,j}^{(q-i)} p_{j-m-1,m}^{(i)} + \sum_{j=1}^{\infty} p_{r,j}^{(q-i)} p_{j-m-2,m}^{(i)}.$$

An index shift and the fact that $p_{j,k}^{(i)} = 0$ if $j \leq 0$ yields

$$(**) = \sum_{j=1}^{\infty} (i p_{r,j+1}^{(q-i)} + p_{r,j+2}^{(q-i)}) p_{j-m,m}^{(i)}.$$

By applying Lemma 2 twice we get
$ip^{(q-i)}_{r,j+1}+p^{(q-i)}_{r,j+2} = ip^{(q-i)}_{r,j+1}+(q-i)p^{(q-i)}_{r,j+1}+p^{(q-i)}_{r-1,j+1} \equiv (q-i)p^{(q-i)}_{r-1,j}+p^{(q-i)}_{r-2,j}\ (q)$.
Using the induction hypothesis we obtain

$$\begin{aligned}(**) &\equiv \sum_{j=1}^{\infty}((q-i)p^{(q-i)}_{r-1,j}+p^{(q-i)}_{r-2,j})p^{(i)}_{j-m,m}\ (q)\\ &\equiv (q-i)p^{(q-i)}_{r-m,m+1}+p^{(q-i)}_{r-m-1,m+1} = p^{(q-i)}_{r-m,m+2}\ (q). \ \blacksquare\end{aligned}$$

In the case of $s = q = 2$ the freedom of choosing the UT generator matrices is very limited.

Proposition 4. *Let $C_1, C_2 \in \mathbb{Z}_2^{\mathbb{N}\times\mathbb{N}}$ be NUT matrices generating a $(0,2)$-sequence. Then $C_2 = PC_1$, where P denotes the first Pascal matrix in base 2.*

Proof. Assume that there is $C_1 \in \mathbb{Z}_2^{\mathbb{N}\times\mathbb{N}}$ (NUT!) such that we can choose two different $C_2, C_2' \in \mathbb{Z}_2^{\mathbb{N}\times\mathbb{N}}$ (both NUT!) such that both C_1, C_2 and C_1, C_2' generate a digital $(0,2)$-sequence. By our assumption that C_2 and C_2' are different we find $c^{(2)}_{i,j}, c'^{(2)}_{i,j}$ with minimal i and then minimal j such that $c^{(2)}_{i,j} \neq c'^{(2)}_{i,j}$. We know that $j \geq i$ since all matrices are UT matrices. We combine the upper left $(j-i)\times j$-submatrix of C_1 with the upper left $i \times j$-submatrix of C_2 to get a non-singular $j \times j$-matrix. If we do the same using C_2' we get another non-singular $j \times j$-matrix which is equal to the one obtained using C_2 except for the bottom right entry. This is not possible in the finite field with just two elements $\mathbb{Z}_2$, so $C_2 = C_2'$. The relation $C_2 = PC_1$ follows since the UT matrices P and I in $\mathbb{Z}_2$ generate a $(0,2)$-sequence. $\blacksquare$

Note that the NUT condition is essential here, since scrambling the Pascal matrices by multiplying by NLT (non-singular lower triangular) matrices from the left has more degrees of freedom for the componentwise choice of the scrambling matrices (see [3] and the references therein).

Furthermore, the following corollary can be deduced from Theorem 4, which is already a consequence of Proposition 2.

Corollary 1. *The first Pascal matrix in base 2 is its own inverse, i.e. $P \cdot P = I \in \mathbb{Z}_2^{\mathbb{N}\times\mathbb{N}}$.*

Proof. By Proposition 4 the matrices I and P are uniquely paired, since both are NUT matrices. If we use P as a (NUT!) scrambling matrix we will get a new pair of NUT matrices PI and PP. By the symmetry of the problem it follows that $PP = I$, as otherwise I, P would not be uniquely paired. $\blacksquare$

In the following we search for generator matrices with lowest possible row lengths in the case of maximal number of dimensions $s = q$. We consider the

$(0, q)$-sequence in prime base q generated by $P^{(0)}, P^{(1)}, \dots, P^{(q-1)} \in \mathbb{Z}_q^{\mathbb{N}\times\mathbb{N}}$ and define a scrambling NUT matrix M columnwise.

Definition 3. We define a matrix $M = (c_1, c_2, \dots, c_d, c_{d+1}, \dots)$, where the dth column, c_d, is given by the following recursion: $c_1 := (1, 0, 0, 0, \dots)^\top$ and

$$c_{d+1} = \left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right) c_d \quad \text{for } d \in \mathbb{N}.$$

Here and below, a zero on top of a matrix in brackets denotes a zero row, and a zero in front denotes a zero column.

Note that by Lemma 2 the recursion above can be given by the following equivalent form:

$$c_{d+1} = P^{(1)} \begin{pmatrix} 0 \\ c_d \end{pmatrix}.$$

First of all we have to check if M is a NUT matrix in order to apply Lemma 1.

Lemma 3. *M defined by Definition 3 is a NUT matrix in $\mathbb{Z}_q$.*

Proof. Denote the dth entry in the lth row of M by $c_{l,d}$. It suffices to prove that $c_{d,d} = 1$ and $c_{l,d} = 0$ if $l > d$. We do this by induction on d.

For $d = 1$ we have $c_{1,1} = 1$ and $c_{l>1,1} = 0$ by the definition of the first column of M.

$d \to d + 1$: Using

$$c_{d+1} = \left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right) c_d$$

we get $c_{l,d+1} = 0$ if $l > d + 1$ and $c_{d+1,d+1} = p^{(1)}_{d,d} c_{d,d} = 1$ by the induction hypothesis and the fact that $P^{(1)}$ is a NUT matrix with all diagonal entries 1. ∎

Theorem 6. *For M given in Definition 3 as scrambling matrix from the right, the matrices $P^{(0)}M, P^{(1)}M, \dots, P^{(q-1)}M$ generate a $(0, q)$-sequence and satisfy*

$$L(\underbrace{0, \dots, 0}_{i-1}, d, 0, \dots, 0) = qd - (i - 1)$$

for all $d \in \mathbb{N}$ and $i \in \{1, \dots, q\}$. Hence the matrices $P^{(0)}M, P^{(1)}M, \dots,$ $P^{(q-1)}M$ have lowest possible row lengths.

To prove Theorem 6 we need further auxiliary results.

Lemma 4. *For every* $k \in \{1, \ldots, q\}$,

$$P^{(q-k)}\left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right)^{k} = \sum_{i=1}^{k} c_{i,k} \begin{pmatrix} \left.\begin{matrix} 0 \\ \vdots \\ 0 \end{matrix}\right\} i \\ I \end{pmatrix} \in \mathbb{Z}_q^{\mathbb{N}\times\mathbb{N}}$$

with some $c_{i,k} \in \{0, 1, \ldots, q-1\}$ *for* $i \in \{1, \ldots, k\}$.

Proof. We prove this by induction.

$k = 1$: Using the equivalent form of the recursion in Definition 3 we obtain

$$P^{(q-1)}\left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right)^{1} I = P^{(q-1)}P^{(1)} \begin{pmatrix} 0 \\ I \end{pmatrix} = \begin{pmatrix} 0 \\ I \end{pmatrix}.$$

$k \to k+1$:

$$\begin{aligned} &P^{(q-k-1)}\left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right)^{k+1} \\ &\quad = P^{(q-k-1)}\left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right)\left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right)^{k} \\ &\quad = P^{(q-k)}\left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right)^{k} + P^{(q-k-1)} \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix} \left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right)^{k}. \end{aligned}$$

By Lemma 2 the following relation is easy to verify:

$$P^{(q-k-1)} = (q-k-1)(0\ \ P^{(q-k-1)}) + \begin{pmatrix} 1 & 0 \\ 0 & P^{(q-k-1)} \end{pmatrix}.$$

Hence
$$P^{(q-k-1)} \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix} = (q-k-1)P^{(q-k)} + \begin{pmatrix} 0 \\ P^{(q-k)} \end{pmatrix}.$$

Using the induction hypothesis we obtain

$$\begin{aligned} &P^{(q-k-1)}\left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right)^{k+1} \\ &\qquad = (q-k)\sum_{i=1}^{k} c_{i,k} \begin{pmatrix} \left.\begin{matrix} 0 \\ \vdots \\ 0 \end{matrix}\right\} i \\ I \end{pmatrix} + \sum_{i=1}^{k} c_{i,k} \begin{pmatrix} \left.\begin{matrix} 0 \\ \vdots \\ 0 \end{matrix}\right\} i+1 \\ I \end{pmatrix} \end{aligned}$$

and the result follows by setting $c_{k+1,k+1} = c_{k,k}$ and $c_{i,k+1} = (q-k)c_{i,k} + c_{i-1,k}$ for $i \le k$, with $c_{0,k} := 0$. ■

Lemma 4 for $k = q$ and induction on n yield the following corollary.

Corollary 2. *For all $n \in \mathbb{N}$,*

$$\left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right)^{nq} = \sum_{i=n}^{qn} c'_{i,n} \left(\begin{array}{c} \left.\begin{matrix} 0 \\ \vdots \\ 0 \end{matrix}\right\} i \\ I \end{array} \right) \in \mathbb{Z}_q^{\mathbb{N}\times\mathbb{N}}$$

with some $c'_{i,n} \in \{0,1,\ldots,q-1\}$ for $i \in \{n,\ldots,qn\}$.

Proof of Theorem 6. We know that $P^{(0)}M,\ldots,P^{(q-1)}M$ generate a $(0,q)$-sequence by Lemma 1, since M is a NUT matrix by Lemma 3. We just have to prove that these matrices have best possible row lengths, i.e.,

$$L(\underbrace{0,\ldots,0}_{i},d,0,\ldots,0) = qd - i$$

for all $d \in \mathbb{N}$ and $i \in \{0,1,\ldots,q-1\}$.

Fix $i \in \{0,1,\ldots,q-1\}$. To guarantee the upper bound on the lengths of the rows it suffices to show that $c_{l,m} = 0$ for all $m \geq ql - i + 1$ where $(c_{l,m})_{l,m\geq 1} := P^{(i)}M$. Therefore, we have to prove that the first $\lfloor (m+i-1)/q \rfloor$ entries of the mth column of $P^{(i)}M$ are zero (here and below, $\lfloor x \rfloor$ denotes the integer part and $\{x\}$ the fractional part of a real x). By Definition 3 the mth column of M is determined by

$$P^{(i)}\left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right)^{m-1} \begin{pmatrix} 1 \\ 0 \\ \vdots \end{pmatrix}.$$

We distinguish the following cases.

$m-1 < q-i$: This is a trivial case since $\lfloor (m+i-1)/q \rfloor = 0$.

$m-1 \geq q-i$: In this case we can apply Lemma 4 and Corollary 2 to get

$$\begin{aligned} &P^{(i)}\left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right)^{m-1} \\ &\quad = P^{(i)}\left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right)^{q-i}\left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right)^{q\lfloor (m+i-1)/q-1\rfloor} \\ &\qquad \times \left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right)^{q\{(m+i-1)/q-1\}} \\ &\quad = \left(\sum_{j=\lfloor (m+i-1)/q\rfloor}^{q\lfloor (m+i-1)/q\rfloor - i} c''(j) \left(\begin{array}{c} \left.\begin{matrix} 0 \\ \vdots \\ 0 \end{matrix}\right\} j \\ I \end{array} \right)\right)\left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right)^{q\{(m+i-1)/q-1\}} \end{aligned}$$

with some $c''(j) \in \{0, 1, \ldots, q-1\}$. Hence the first column of the resulting matrix contains at least $\lfloor (m+i-1)/q \rfloor$ zero entries at the top, and the result follows. ∎

Remark 3. Note that for base 2 the cases $s = 2$ and $s = q$ are equal. In this case, M as defined in Theorem 5 equals the scrambling matrix M given in Definition 3:

$$M = \begin{pmatrix} \mathrm{col}_1^{(1)} & \mathrm{col}_2^{(1)} & \begin{pmatrix} 0 \\ \mathrm{col}_2^{(1)} \end{pmatrix} & \begin{pmatrix} 0 \\ \mathrm{col}_3^{(1)} \end{pmatrix} & \begin{pmatrix} 0 \\ 0 \\ \mathrm{col}_3^{(1)} \end{pmatrix} & \begin{pmatrix} 0 \\ 0 \\ \mathrm{col}_4^{(1)} \end{pmatrix} & \ldots \end{pmatrix}.$$

This can be easily checked using the equivalent form of the recursion in Definition 3 and the statements in Proposition 3.

We recall the two-dimensional case as considered in Theorem 5 and discover symmetries concerning the generator matrices with lowest possible row lengths. One is the relation between the generator matrices M and $P^{(i)}M$:

$$P^{(i)}M = \begin{pmatrix} 1 & 0 & 0 & \ldots \\ 0 & & & \\ 0 & & \overline{M} & \\ \vdots & & & \end{pmatrix}.$$

Furthermore, we get repetition at the "edges", i.e. the column just before and the column for which the number of zeros at the top increases by one are equal except for "adding a zero shift".

For the case where the dimension is equal to the base we find similar symmetries given in the following remark. These properties could be useful in case of implementation.

Remark 4. For the sequence generated by $P^{(0)}M, P^{(1)}M, \ldots, P^{(q-1)}M$, where M is the scrambling matrix given in Definition 3, we achieve a symmetry concerning $M = P^{(0)}M$ and $P^{(q-1)}M$ similar to the two-dimensional case:

$$P^{(q-1)}M = \begin{pmatrix} 1 & 0 & 0 & \ldots \\ 0 & & & \\ 0 & & M & \\ \vdots & & & \end{pmatrix}.$$

If we take a look at the "edges" in the matrices $P^{(0)}M, \ldots, P^{(q-1)}M$, we discover repetitions as in the two-dimensional case. For every $i \in \{0, 1, \ldots, q-1\}$ the following relation holds for all $n \in \mathbb{N}$:

$$\begin{pmatrix} 0 \\ c_{nq-i}^{(i)} \end{pmatrix} = c_{nq-i+1}^{(i)},$$

where $c_m^{(i)}$ denotes the mth column of $P^{(i)}M$.

Proof. The symmetry concerning $M = P^{(0)}M$ and $P^{(q-1)}M$ can be easily checked using the equivalent form of the recursion in Definition 3 which immediately implies

$$P^{(q-1)}c_{d+1}^{(0)} = \begin{pmatrix} 0 \\ c_d^{(0)} \end{pmatrix}.$$

For the proof of the repetition at the "edges" we recall the following terms as considered in the proof of Theorem 6:

$$P^{(i)}\left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right)^{q-i} \left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right)^{q\lfloor (m+i-1)/q-1 \rfloor} \times \left(P^{(1)} + \begin{pmatrix} 0 \\ P^{(1)} \end{pmatrix}\right)^{q\{(m+i-1)/q-1\}}.$$

By Lemma 4 and Corollary 2 the leading terms can be written as a special linear combination of shifted unit matrices, hence it suffices to prove the repetition at the first "edge" in M, which can be done by verifying

$$\begin{pmatrix} 0 \\ c_q^{(0)} \end{pmatrix} = c_{q+1}^{(0)}. \tag{8}$$

If we prove that $c_q^{(0)}$ is of the form $(q-1, \underbrace{0, \ldots, 0}_{q-2}, 1, 0, \ldots)^\top$, then (8) will follow:

$$\begin{aligned} c_{q+1}^{(0)} = P^{(1)} \begin{pmatrix} 0 \\ c_q^{(0)} \end{pmatrix} &= (q-1)\mathrm{col}_2^{(1)} + \mathrm{col}_{q+1}^{(1)} \\ &= (q-1, q-1, 0, \ldots)^\top + (1, \underbrace{0, \ldots, 0}_{q-1}, 1, 0, \ldots)^\top = \begin{pmatrix} 0 \\ c_q^{(0)} \end{pmatrix}. \end{aligned}$$

It remains to prove that $c_q^{(0)}$ has the above form. By the restriction on the lengths of the rows in $P^{(i)}M$ the vector $c_q^{(0)}$ has to solve the following system of congruences:

$$D \cdot (x_1, x_2, \ldots, x_{q-1}, 1, 0, \ldots)^\top = (0, \ldots, 0)^\top \in \mathbb{Z}_q^{q-1}$$

where D is the $(q-1) \times \mathbb{N}$-matrix in $\mathbb{Z}_q$ formed by the first row of $P^{(1)}$, the first row of $P^{(2)}, \ldots$ and the first row of $P^{(q-1)}$.

Since $P^{(1)}, \ldots, P^{(q-1)}$ generate a $(0, q-1)$-sequence, the left $(q-1) \times (q-1)$-submatrix of D has full rank. Thus there exists a unique solution in the finite field $\mathbb{Z}_q$. We verify that

$$(q-1, \underbrace{0, \ldots, 0}_{q-2}, 1, 0, \ldots)^\top$$

solves the system above, by the following computation for $i \in \{1, \ldots, q-1\}$:

$$(q-1)p_{1,1}^{(i)} + p_{1,q}^{(i)} = (q-1)\binom{0}{0}i^0 + \binom{q-1}{0}i^{q-1} \equiv (q-1) + 1 \equiv 0 \ (q). \ \blacksquare$$

Acknowledgments. R. Hofer was a recipient of a DOC-fFORTE-fellowship of the Austrian Academy of Sciences at the Institute of Financial Mathematics at the University of Linz (Austria).

G. Larcher was supported by the Austrian Science Foundation (FWF), Project P21196.

References

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

[2] H. Faure, *Discrépance de suites associées à un système de numération (en dimension s)*, Acta Arith. 41 (1982), 337–351.

[3] H. Faure and S. Tezuka, *Another random scrambling of digital (t,s)-sequences*, in: K. T. Fang et al. (eds.), Monte Carlo and Quasi-Monte Carlo Methods 2000, Springer, Berlin, 2002, 242–256.

[4] R. Hofer, *On the distribution properties of Niederreiter–Halton sequences*, J. Number Theory 129 (2009), 451–463.

[5] —, *On subsequences of Niederreiter–Halton sequences*, in: Monte Carlo and Quasi-Monte Carlo Methods 2008, to appear.

[6] R. Hofer, P. Kritzer, G. Larcher and F. Pillichshammer, *Distribution properties of generalized van der Corput–Halton sequences and their subsequences*, Int. J. Number Theory 5 (2009), 719–746.

[7] D.-H. Kim, *On the joint distribution of q-additive functions in residue classes*, J. Number Theory 74 (1998), 307–336.

[8] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley, New York, 1974.

[9] G. Larcher and H. Niederreiter, *Generalized (t,s)-sequences, Kronecker-type sequences, and Diophantine approximations of formal Laurent series*, Trans. Amer. Math. Soc. 347 (1995), 2051–2073.

[10] D. J. Newman, *On the number of binary digits in a multiple of three*, Proc. Amer. Math. Soc. 21 (1969), 719–721.

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

[12] I. M. Sobol', *On the distribution of points in a cube and the approximate evaluation of integrals*, USSR Comput. Math. Math. Phys. 7 (1967), 86–112.

[13] C. Xing and H. Niederreiter, *A construction of low-discrepancy sequences using global function fields*, Acta Arith. 73 (1995), 87–102.

Roswitha Hofer, Gerhard Larcher
Institute of Financial Mathematics
University of Linz
Altenbergerstr. 69
A-4040 Linz, Austria
E-mail: roswitha.hofer@jku.at
gerhard.larcher@jku.at

Received on 19.2.2009
and in revised form on 4.5.2009 (5948)