Uniform Distribution Theory **6** (2011), no.2, 13–30

uniform
distribution
theory

AN EXPLICIT CONSTRUCTION OF FINITE-ROW DIGITAL $(0, s)$-SEQUENCES

Roswitha Hofer and Gottlieb Pirsic

ABSTRACT. In this paper we revisit the finite-row $(0, s)$-sequences as introduced by Hofer and Larcher, in particular those constructed by a scrambling of the Faure sequence. We give a simple explicit formula based on the Stirling numbers (of the first kind) for the scrambling matrices. This explicit formula provides more insight into the (somewhat peculiar) recursively defined scrambling matrix used in the constructions of Hofer and Larcher and also into the corresponding finite-row generator matrices. It is then applied to the investigation of the self-similar structure of the generator matrices and to efficient generation of the sequence.

Communicated by Robert F. Tichy

1. Introduction

In many applications, e.g., simulation, digital imaging, financial mathematics, one is interested in accurately approximating numerically the integral of a function $f : [0, 1]^s \to \mathbb{R}$,

$$I_s(f) := \int_{[0,1]^s} f(\boldsymbol{x}) \mathrm{d}\boldsymbol{x},$$

where the integration domain may be very high-dimensional, having perhaps hundreds of dimensions. One way of accomplishing this task is to use a *quasi-Monte Carlo* (QMC) rule such as

$$Q_{N,s}(f) := \frac{1}{N} \sum_{n=0}^{N-1} f(\boldsymbol{x}_n),$$

2010 Mathematics Subject Classification: 11K31, 11K38, 11B73.
Keywords: Stirling numbers, low-discrepancy sequences, finite-row digital $(0, s)$-sequences.
The first author was supported by the Austrian Science Fund (FWF), Project P21943. The second author was supported by the Austrian Science Fund (FWF), S9609.

where $(\boldsymbol{x}_n)_{n=0}^{N-1}$ is a finite sequence (or the initial terms of an infinite sequence) of a deterministic point set in $[0,1)^s$. It is well-known in the theory of QMC methods, that the so-called *low-discrepancy* point sets and sequences yield a low integration error when a QMC algorithm is used (see, among many others, [1, 2, 8, 10, 13]).

One of the most widespread and powerful techniques to construct low-discrepancy point sequences in the s-dimensional unit cube is the concept of digital (t,s)-sequences (see e.g. [11, 13]) or, more general, digital $(\mathbf{T},s)$-sequences (see [9]). In this paper we restrict ourselves to the special case of digital $(0,s)$-sequences (this corresponds to the best possible asymptotic order for the upper bound of discrepancy).

We recall the *digital method*:

Definition 1. *Let $s \geq 1$ denote the dimension and let q be a prime. Further let $C_1,\ldots,C_s$ be $\mathbb{N}\times\mathbb{N}$-matrices over the finite field $\mathbb{F}_q$. We construct a sequence $(\boldsymbol{x}_n)_{n\geq 0}$, $\boldsymbol{x}_n = \left(x_n^{(1)},\ldots,x_n^{(s)}\right)$, $n\in\mathbb{N}_0$, by generating the jth coordinate of the nth point, $x_n^{(j)}$, as follows. We represent $n = n_0 + n_1 q + n_2 q^2 + \cdots$ in base q and set*

$$C_j \cdot (n_0, n_1, \ldots)^\top =: \left(y_1^{(j)}, y_2^{(j)}, \ldots\right)^\top \in {\mathbb{F}_q}^{\mathbb{N}}$$

and

$$x_n^{(j)} := \frac{y_1^{(j)}}{q} + \frac{y_2^{(j)}}{q^2} + \cdots .$$

(Note that since q is prime we can identify the elements of $\mathbb{F}_q$ with residue classes modulo q; also, we do not distinguish the residue classes from their representatives $\{0,1,\ldots,q-1\}$.)

The sequence generated by the matrices $C_1,\ldots,C_s$ is called a digital $(0,s)$-sequence over $\mathbb{F}_q$ *if for every $m\in\mathbb{N}$ and for all $d_1,d_2,\ldots,d_s\in\mathbb{N}_0$ with $d_1+\cdots+d_s = m$ the $(m\times m)$-matrix whose rows consist of the rows of each upper left $(d_i\times m)$-submatrix of C_i, for $i=1,\ldots,s$, has full rank m.*

Note that the condition on the rank structure of the generator matrices sketched above is very restrictive. E.g. it is known that such special generator matrices can only exist if the dimension s is at most equal to the base q (see e.g. [13]). One famous example of digital $(0,s)$-sequences was given by Faure in [3]:

Example 1 (Faure sequences). *Let q be a prime. For $i \in \{0,1,\dots,q-1\}$ we define the i th Pascal matrix in base q by $P^{(i)} := (p^{(i)}_{k,j})_{k,j\geq 1}$,*

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

modulo q, where $k \in \mathbb{Z}, j \in \mathbb{N}$ and $0^0 := 1$. Then the matrices $P^{(0)}, \cdots, P^{(q-1)}$ generate a digital $(0,q)$-sequence in base q.

For $q = 2$ this sequence had been given earlier by Sobol [14]*. A development to increasingly more general versions has been made e.g. in* [11, 12, 13, 15]*.*

In [6] the question was posed, if there exist matrices where in each row only finitely many entries are nonzero, while the above rank-structure conditions are still satisfied, and the notion of *finite-row generator matrices* was introduced. This question was raised during the investigation of the discrepancy of the so called Niederreiter-Halton sequences which are built by juxtaposing the components of digital $(\mathbf{T}, s)$-sequences in different prime bases. E.g., the 5-dimensional sequence where the first two components are given by the Faure sequence in base 2 and the remaining three components are given by the Faure sequence in base 3 is an example of a Niederreiter-Halton sequence. The idea of constructing multi-dimensional sequences by combining the components of digital sequences in different prime bases is motivated by the special properties of the so called Halton sequences (introduced in [5]). A Halton sequence is built by juxtaposing van der Corput sequences, which are special digital $(0,1)$-sequences, in different prime bases and surprisingly the multi-dimensional sequence constructed that way is also a low-discrepancy sequence. Of course a natural question is to ask if there are more examples of digital sequences that can be used as components of Niederreiter-Halton sequences, resulting in a good low-discrepancy sequence. Unfortunately not all digital $(0,s)$-sequences have good mixing properties concerning the low-discrepancy property. For example in [6] it was shown that the discrepancy of the 5-dimensional sequence from above satisfies quite large lower bounds. Altogether the results obtained in [6] for certain different classes of Niederreiter-Halton sequences suggested to combine digital $(0,s)$-sequences that are generated by matrices consisting of rows with as few as possible nonzero entries. This motivated the investigation of the finite-row generator matrices.

Of course the restrictive condition on the rank structure forces the matrices to contain a certain amount of nonzero entries. In [6] it was shown that in the best possible case for every $d > 0$, $i \in \{1,\dots,s\}$ the dth row of C_i should have a length of $sd + 1 - \pi(i)$, for some permutation π on $\{1,\dots,s\}$. In this case we say that the matrix has *shortest possible row length in the sense of Hofer and Larcher*.

From the following Proposition by Faure and Tezuka in [4] it is easy to deduce the existence of such *finite-row* $(0,s)$*-sequences.*

Proposition 1. *Let* $C_1, \ldots, C_s \in \mathbb{F}_q^{\mathbb{N}\times\mathbb{N}}$ *be the generator matrices of a digital* $(0,s)$*-sequence in prime base* $q \geq s$*. If* M *is a non-singular upper triangular (NUT) matrix over* $\mathbb{F}_q$*, then the matrices* $C_1M, \ldots, C_sM$ *generate a digital* $(0,s)$*-sequence in prime base* $q \geq s$*.*

The strategy is to determine for given generator matrices $C_1, \ldots, C_s$ a suitable matrix M column by column, by solving systems of equations related to the restrictions on the row lengths. Note that the matrix multiplication with a NUT matrix from the right in effect is a special rearrangement of the sequence; in order to find a suitable rearrangement by the strategy above, one has to solve systems of equations. We refer the interested reader to [6] for more details.

Since for the Faure sequence in any prime base q very simple explicit formulas for the generator Pascal matrices are known (compare Example 1) it is natural to ask for a more effective way to compute a proper NUT matrix M which goes along with the Pascal matrices. In [6] a recursion for such a scrambling matrix M was discovered: set

$$c_1 := (1,0,0,0,\ldots)^\top, \quad c_{d+1} = P^{(1)} \begin{pmatrix} 0 \\ c_d \end{pmatrix},$$

for $d \in \mathbb{N}$. Then $M := (c_1, c_2, c_3, \ldots)$.

Note that from the fact that $P^{(i)} = (P^{(1)})^i$ it is easy to check that the matrix $P^{(q-1)}M =: S$ can also be produced by the recursion

$$c_1 := (1,0,0,0,\ldots)^\top, \quad c_{d+1} = \begin{pmatrix} 0 \\ P^{(1)}c_d \end{pmatrix}$$

for $d \in \mathbb{N}$. Hence S is also an appropriate scrambling matrix to obtain a finite-row $(0,q)$-sequence.

In this paper we prove an explicit formula for the matrix S in Section 2.1, viz.,

$$S = \left(\begin{bmatrix} j-1 \\ k-1 \end{bmatrix} \right)_{k,j\geq 1}$$

modulo q, where $\left[{m \atop n}\right]$ is the Karamata notation for the unsigned Stirling number of the first kind (note the striking similarity of S to the first Pascal matrix $(\binom{j-1}{k-1})_{k,j\geq 1})$ modulo q. There exist several equivalent definitions for $\left[{m \atop n}\right]$, e.g., as the number of permutations of m elements with n cycles or by a recursion.

From this explicit formula we are able to derive further interesting properties of the finite-row generator matrices and also of the associated digital $(0,q)$-sequence. In Section 2.2 we determine for $N = q^{q\cdot m}, m \in \mathbb{N}$ a special permutation

π of $\{0,1,\cdots,q^{q\cdot m}-1\}$ that can be applied towards efficient generation of the sequence in the following way: for the first N points of the sequence it suffices to compute the first component, while the other components result from applying the permutation, i.e.,

$$\boldsymbol{x}_n = (x_n^{(1)}, x_{\pi(n)}^{(1)}, \ldots, x_{\pi^{q-1}(n)}^{(1)}), n = 0,1,\ldots,N-1.$$

Furthermore, we show a self-similar structure of the finite-row generator matrices in Section 2.3. We conclude the paper with some open problems as outlook to further research in Section 3.

2. Results

Let q be a given prime base. We define matrices $M(a), S_1(a) \in \mathbb{F}_q{}^{\mathbb{N}\times\mathbb{N}}$ where $a \in \{1,\ldots,q-1\}$. The matrix $M(a)$ shall be defined by its columns, i.e., we set

$$c_1 := (1,0,0,0,\ldots)^T \in \mathbb{F}_q{}^{\mathbb{N}}, \quad c_{d+1} := \begin{pmatrix} 0 \\ P^{(a)} \cdot c_d \end{pmatrix},$$

for $d \in \mathbb{N}$, where $P^{(a)}$ is the ath Pascal matrix defined in Example 1. Then $M(a) := (c_1, c_2, c_3, \ldots)$.

2.1. An explicit formula for the matrix

Set $S_1(a) := (\begin{bmatrix} j-1 \\ i-1 \end{bmatrix} a^{j-i})_{i,j\geq 1}$ modulo q, where $\begin{bmatrix} n \\ k \end{bmatrix}$ denotes the *unsigned* Stirling number of the first kind, defined by:

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1)\begin{bmatrix} n-1 \\ k \end{bmatrix}, \quad \text{for } k,n \in \mathbb{N} \tag{1}$$

with initial values $\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1$ and $\begin{bmatrix} n \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ n \end{bmatrix} = 0$ for all $n > 0$.

Theorem 1. *We have $M(a) = S_1(a)$.*

Proof. We prove the equality by induction on the columns.

First we observe that the equality holds for the initial column vector:

$$c_1 = (1,0,0,\ldots)^T = (\begin{bmatrix} 0 \\ 0 \end{bmatrix} a^0, \begin{bmatrix} 0 \\ 1 \end{bmatrix} a^{-1}, \begin{bmatrix} 0 \\ 2 \end{bmatrix} a^{-2}, \ldots)^T.$$

For the induction step we assume that

$$c_d = (\begin{bmatrix} d-1 \\ 0 \end{bmatrix} a^{d-1}, \begin{bmatrix} d-1 \\ 1 \end{bmatrix} a^{d-2}, \begin{bmatrix} d-1 \\ 2 \end{bmatrix} a^{d-3}, \ldots)^T$$

and compute

$$\begin{aligned} c_{d+1} &= \begin{pmatrix} 0 \\ P^{(a)} \cdot c_d \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ \left(\sum_{j\geq 1} \binom{j-1}{i-1} a^{j-i} \begin{bmatrix} d-1 \\ j-1 \end{bmatrix} a^{d-j}\right)^T_{i\geq 1} \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ \left(a^{d-i} \sum_{j\geq 1} \binom{j-1}{i-1} \begin{bmatrix} d-1 \\ j-1 \end{bmatrix}\right)^T_{i\geq 1} \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ \left(a^{d-i} \begin{bmatrix} d \\ i \end{bmatrix}\right)^T_{i\geq 1} \end{pmatrix}, \end{aligned}$$

where for the last step we used the equality

$$\sum_{j\geq 0} \binom{j}{i} \begin{bmatrix} d \\ j \end{bmatrix} = \begin{bmatrix} d+1 \\ i+1 \end{bmatrix},\ d, i \geq 0,$$

which can be found e.g., in [7, chapter 1.2.6.]. Finally the fact that $\begin{bmatrix} d \\ 0 \end{bmatrix} a^d = 0$ for $d \in \mathbb{N}$ yields the desired result

$$c_{d+1} = \left(\begin{bmatrix} d+1-1 \\ 0 \end{bmatrix} a^{d+1-1}, \begin{bmatrix} d+1-1 \\ 1 \end{bmatrix} a^{d+1-2}, \begin{bmatrix} d+1-1 \\ 2 \end{bmatrix} a^{d+1-3}, \dots\right)^T.$$

□

2.2. Relations between the generator matrices and a componentwise construction based on special permutations

Now we use the matrix $S_1(a)$ as scrambling matrix in application of Proposition 1. This gives the matrices $P^{(0)}S_1(a)$, $P^{(1)}S_1(a), \dots,$ $P^{(q-1)}S_1(a)$ generating a digital $(0, q)$-sequence.

The following theorem shows an interesting property of these matrices. We determine very thin band matrices $Q(a, b)$, such that $P^{(b)} \cdot S_1(a) = S_1(a) \cdot Q(a, b)$, which implies that for each choice of $a \in \{1, \dots, q-1\}$ the scrambled matrices have shortest possible row lengths in the sense of Hofer and Larcher.

Theorem 2. *We have*

$$P^{(b)} \cdot S_1(a) = S_1(a) \cdot Q(a, b),$$

where

$$Q(a, q-a) = Q(a) := \left(\delta_{k,j} - a(j-1)\delta_{k,j-1}\right)_{k,j\geq 1},$$

$$Q(a,b) := Q(a)^l = \left((-a)^{j-k}\binom{j-1}{k-1}(l)_{j-k}\right)_{k,j\geq 1},$$

for $l(q-a) \equiv b \pmod q$. (For integers m, n, the notation $(n)_m$ refers to the falling factorial $n(n-1)\cdots(n-m+1)$, empty products equal 1, also for $n = 0$.)

The matrices $Q(a)^l$ are band matrices with bandwidth $l+1$ for $1 \leq l < q$ and $Q(a)^q \equiv (\delta_{k,j})_{k,j\geq 1}$ modulo q.

For the proof of the theorem we make use of the Stirling numbers of the second kind $\left\{ {n \atop k} \right\}$, $n, k \in \mathbb{N}$, which have a combinatorial interpretation as the number of ways to partition a set of n objects into k groups. They obey the recurrence relation (which may be taken as an alternative definition)

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k\left\{ {n-1 \atop k} \right\}, \text{ for } n, k \in \mathbb{N}$$

with the initial values $\left\{ {0 \atop 0} \right\} = 1$ and $\left\{ {n \atop 0} \right\} = \left\{ {0 \atop n} \right\} = 0$ for any integer $n > 0$.

By the combinatorial interpretation or, indeed, the recursion it is not immediately obvious (but a well-known fact in combinatorics) that the Stirling numbers of the first and the second kind are in an inversion relation to each other. Introducing a small generalization, the following holds.

Lemma 1. *We have $S_2(a)S_1(a) = S_1(a)S_2(a) = I$, where*

$$S_2(a) = \left(\left\{ {j-1 \atop k-1} \right\}(-a)^{j-k}\right)_{k,j\geq 1} \quad \textit{and } I = (\delta_{k,j})_{k,j\geq 1}.$$

Proof. Follows immediately from the relation $S_1(1)S_2(1) = S_2(1)S_1(1) = I$ that can be found e.g., in [7, Ch.1.2.6]. □

The proof of the theorem builds from the case $l = 1$, which we present in this lemma.

Lemma 2. *We have*

$$S_2(a) \cdot P^{(q-a)} \cdot S_1(a) = Q(a, q-a) =: Q(a) = \left(\delta_{i,j} - a(j-1)\delta_{i,j-1}\right)_{i,j\geq 1}.$$

Proof. Note that from the recursive definition of $M(a)$ and from Theorem 1 it is easy to see that $P^{(a)} \cdot S_1(a) = \left(\left[{j \atop k} \right] a^{j-k}\right)_{k,j\geq 1}$ modulo q.

Now the result is easily deduced from

$$\left((S_2(a) \cdot P^{(q-a)})^{-1}\right)^{-1} = (P^{(a)} \cdot S_1(a))^{-1} = \left(\left(\left[{j \atop k} \right] a^{j-k}\right)_{k,j\geq 1}\right)^{-1}$$

$$= \left(\left\{ \begin{matrix} j \\ k \end{matrix} \right\} (-a)^{j-k} \right)_{k\geq 1, j\geq 1}$$

modulo q and

$$\left(\left\{ \begin{matrix} j \\ k \end{matrix} \right\} (-a)^{j-k} \right)_{k,j\geq 1} = \left(\left\{ \begin{matrix} j-1 \\ k-1 \end{matrix} \right\} (-a)^{j-k} - ak \left\{ \begin{matrix} j-1 \\ k \end{matrix} \right\} (-a)^{j-1-k} \right)_{k,j\geq 1}.$$

□

Proof of Theorem 2.
For any $b \in \{0, \dots, q-1\}$ we choose $l \in \{0, 1, \dots, q-1\}$ such that $l(q-a) \equiv b \pmod{q}$, so that $P^{(b)} = (P^{(q-a)})^l$. Then Lemma 2 yields

$$P^{(b)} S_1(a) \quad = \quad S_1(a) \big(S_2(a) \cdot P^{(q-a)} \cdot S_1(a) \big)^l = S_1(a) Q(a)^l.$$

We denote the ith unit vector of $\mathbb{F}_q^{\mathbb{N}}$ by e_i. From the form of $Q(a)$ in Lemma 2 we know, that $Q(a)$ maps e_i to $e_i - a(i-1)e_{i-1}$. So, by induction

$$Q(a)^l = \left(\sum_{n=0}^{l} \delta_{k,j-n} (-a)^n \binom{l}{n} (j-1)_n \right)_{k,j\geq 1}.$$

Finally it is easy to check that

$$\begin{aligned} \sum_{n=0}^{l} \delta_{k,j-n} (-a)^n \binom{l}{n} (j-1)_n &= (-a)^{j-k} \binom{l}{j-k} (j-1)_{j-k} \\ &= (-a)^{j-k} \binom{j-1}{k-1} (l)_{j-k}. \end{aligned}$$

□

Corollary 1. *The matrices $S_1(a), S_1(a)Q(a), \dots, S_1(a)Q(a)^{q-1}$ are generator matrices of a digital $(0, s)$-sequence and have shortest possible row lengths in the sense of Hofer and Larcher.*

Furthermore, to construct the first q^{qv} points of the sequence it suffices to compute the first component by matrix-vector multiplication, the subsequent components are generated by repeated application of a permutation of indices, i.e.,

$$\boldsymbol{x}_n = (x_n^{(1)}, x_{\pi_v(n)}^{(1)}, \dots, x_{\pi_v^{q-1}(n)}^{(1)}).$$

The permutation π_v acting on $\{0, \dots, q^{qv} - 1\}$ here can in fact be reduced to a permutation π_1 acting on $\{0, \dots, q^q - 1\}$ via q^q-adic digits, i.e., given a representation of $k = \sum_{r=1}^{v-1} k_r q^{qr}$, $0 \le k_r < q^{qn}$, we have

$$\pi_v(k) = \sum_{r=1}^{v-1} \pi_1(k_r) q^{qr}.$$

Proof. Theorem 2 and Proposition 1 yield that the matrices generate a digital $(0, s)$-sequence. From the defining recurrence (1) it is easy to deduce that $\left[{n \atop k}\right]$ is divisible by q for all $k, n \in \mathbb{N}$ such that $n > qk$ (e.g., by induction on k). Hence the dth row of $S_1(a)$ has length less than or equal to $q(d-1)+1$. This together with the fact that $Q(a)$ is a band matrix with bandwidth 2 implies the conditions on the row lengths, in fact we get that the dth row of $S_1(a)Q(a)^l$ for $l \in \{0, 1, \dots, q-1\}$ has length less than or equal to $qd - (q - 1 - l)$. Hence these matrices have shortest possible row lengths in the sense of Hofer and Larcher.

To conclude the proof we note that the form of $Q(a)$ given in the Theorem is actually a block diagonal matrix, i.e.,

$$Q(a) = \begin{pmatrix} B & 0 & 0 & \cdots \\ 0 & B & 0 & \cdots \\ \vdots & 0 & \ddots & \cdots \\ \vdots & \vdots & \ddots & \ddots \end{pmatrix}$$

with

$$B = \begin{pmatrix} 1 & (q-1)a & 0 & \cdots & \cdots \\ 0 & 1 & (q-2)a & 0 & \cdots \\ \vdots & 0 & \ddots & \ddots & \ddots \\ \vdots & \vdots & 0 & 1 & a \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} \in \mathbb{F}_q{}^{q \times q},$$

and hence $Q(a)$ operates on each of the consecutive blocks of length q in the vector $(n_0, n_1, \dots)^T$ and the blockwise operation π_1 is determined by B. Thus the assertions on π_v follow. □

Example 2. *For $q = 2$ the upper left submatrix $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Hence $\pi_1 : \{0, 1, 2, 3\} \to \{0, 1, 2, 3\}$ equals the transposition $(2, 3)$ and the first four points of the sequence are $(x_0^{(1)}, x_0^{(1)}), (x_1^{(1)}, x_1^{(1)}), (x_2^{(1)}, x_3^{(1)}), (x_3^{(1)}, x_2^{(1)})$. If we want to compute the first $2^{2 \cdot 2} = 16$ points we apply π_1 to each string of $2^2 = 4$ points and then π_1 to the 4 strings:*

$$\begin{array}{cccc} (0,1,2,3) & (4,5,6,7) & (8,9,10,11) & (12,13,14,15) \\ \downarrow \pi_1 & \downarrow \pi_1 & \downarrow \pi_1 & \downarrow \pi_1 \\ \underbrace{(0,1,3,2)}_{a} & \underbrace{(4,5,7,6)}_{b} & \underbrace{(8,9,11,10)}_{c} & \underbrace{(12,13,15,14)}_{d} \\ & & \downarrow \pi_1 & \\ \overbrace{(0,1,3,2)}^{a} & \overbrace{(4,5,7,6)}^{b} & \overbrace{(12,13,15,14)}^{d} & \overbrace{(8,9,11,10)}^{c} \end{array}$$

or, in cyclic notation, $(3,4)(6,7)(8,12)(9,13)(10,15)(11,14)$.

Remark 1. *In principle, by* $P^{(i)} = (P^{(1)})^i$, *we can also generate the first* $q^{qv}, v \in \mathbb{N}$ *points of the Faure sequence by repeated application of a permutation* $\overline{\pi}_v : \{0,1,\ldots,q^{qv}-1\} \to \{0,1,\ldots,q^{qv}-1\}$, *such that*

$$\boldsymbol{x}_n = (x_n^{(1)}, x_{\overline{\pi}_v(n)}^{(1)}, \ldots, x_{\overline{\pi}_v^{q-1}(n)}^{(1)}).$$

However, the permutation cannot be computed digitwise in base q^q *representation and does not have a similarly transparent and quick-to-implement structure. To illustrate,* $\overline{\pi}_2$ *in base* 2 *is given by*

$$\begin{array}{cccccccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 1 & 3 & 2 & 5 & 4 & 6 & 7 & 15 & 14 & 12 & 13 & 10 & 11 & 9 & 8 \end{array}$$

or in cyclic notation $(2,3)(4,5)(8,15)(9,14)(10,12)(11,13)$.

2.3. The self-similar structure of the generator matrices

The Pascal matrices (i.e., binomial coefficients modulo a prime) have a well-known and appealing self-similar structure (see Figure 1) that is explained by Lucas' Theorem on binomial coefficients.

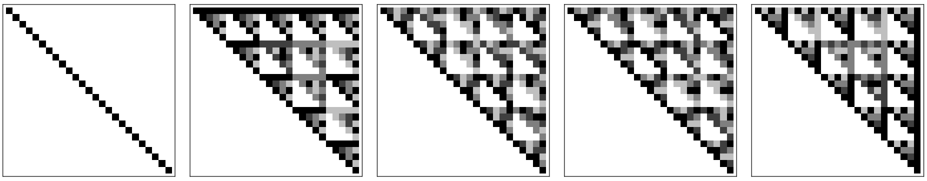

Figure 1. The Pascal matrices in base 5, upper left 25×25 submatrices.

Proposition 2. *Let* q *be prime and* $m, n \in \mathbb{N}_0$. *With* $m = m_1 q + m_0$ *and* $n = n_1 q + n_0$, $0 \leq m_0, n_0 < q$ *and the base* q *representations* $m = \sum_{i \geq 0} \mu_i q^i, n =$

$\sum_{i\geq 0}\nu_i q^i$ *we have*

$$\binom{m}{n} \equiv \binom{m_0}{n_0}\binom{m_1}{n_1} \equiv \prod_{i\geq 0}\binom{\mu_i}{\nu_i} \pmod q \quad \text{‘Lucas’ Theorem’}$$

and

$$p^{(b)}_{m,n} = p^{(b)}_{m_0,n_0}\cdot p^{(b)}_{m_1,n_1} = \prod_{i\geq 0} p^{(b)}_{\mu_i,\nu_i} \in \mathbb{F}_q.$$

Proof. Lucas’ Theorem can be found e.g., as an exercise in [7, Ch.1.2.6]. From the fact that $b^{q-1}\equiv 1 \pmod q$ for all $b\in\{1,\dots,q-1\}$ it is easy to deduce the formula for the Pascal matrices. For $b=0$, $\delta_{m,n}=\delta_{m_0,n_0}\delta_{m_1,n_1}$ holds trivially. □

The preceding proposition can be visualized as follows. Consider a partition of a Pascal matrix into $q\times q$ submatrices. Then any submatrix of index (m_1,n_1) is a copy of the $(0,0)$-submatrix, adjusted by a binomial factor $\binom{m_1}{n_1}$ modulo q. By induction, the same holds also for a partition into $q^i\times q^i$ submatrices for $i>1$.

In the following proposition we give a similar reduction formula for Stirling numbers of the first kind. It is not quite as simple as for binomial coefficients but still serves to explain the self-similar structure of the finite-row generator matrices in Theorem 3 (see Figure 2).

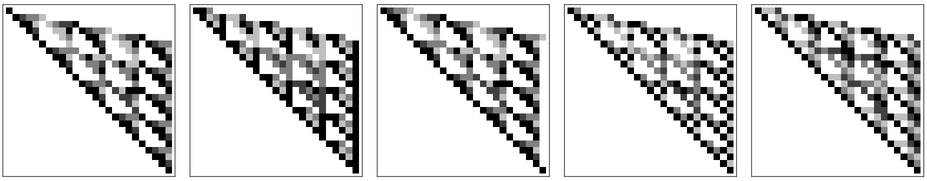

FIGURE 2. The matrices $P^{(i)}S_1(2)$ in base 5, upper left 25×25 submatrices.

PROPOSITION 3. *For $n,m\geq 0$,*

$$a^{n-m}\begin{bmatrix} n\\ m\end{bmatrix} \equiv a^{n_0-m_0}\begin{bmatrix} n_0\\ m_0\end{bmatrix} \times (-1)^{n_1-m_1}\begin{cases}(-1)\binom{n_1}{m_1-1} & \text{if } n_0=q-1, m_0=0,\\ \binom{n_1}{m_1} & \text{else}\end{cases} \pmod q,$$

where

$$\begin{aligned} n &= n_1 q + n_0, \quad 0 \leq n_0 < q, \\ m - n_1 &= m_1(q-1) + m_0, \quad 0 \leq m_0 < q-1. \end{aligned}$$

(Note that for $q = 2$ the formula also holds, with $m_1 = m - n_1$, $m_0 = 0$. See also Example 3 below.)

Proof. We start by observing that for prime q we have

$$a^{n-m} = a^{n_0+n_1q-m_1(q-1)-m_0-n_1} \equiv a^{n_0-m_0} \pmod q,$$

so a plays no role in the rest of the proof.

The main tool of the proof is that the 'rising factorial' function is a generating function for $\left[{n \atop m}\right]$ in the following sense: with the usual coefficient extraction operator notation, $[x^m]$, we have

$$\begin{bmatrix} n \\ m \end{bmatrix} = [x^m](x)^{(n)}, \qquad \text{where } (x)^{(n)} := x(x+1)\cdots(x+n-1).$$

First we note that with $n = n_0 + \sum_{i>0} \nu_i q^i$,

$$(x)^n \equiv (x)^{(n_0)}(x)^{(\nu_1 q)}(x)^{(\nu_2 q^2)} \cdots \pmod q.$$

Furthermore, for any $i > 0$

$$(x)^{(\nu_i q^i)} \equiv \left((x)^{(q)}\right)^{\nu_i q^{i-1}} \pmod q,$$

hence

$$(x)^{(n)} \equiv (x)^{(n_0)}\left((x)^{(q)}\right)^{n_1} \pmod q.$$

Regarding the expression $(x)^{(q)}$ we observe that it is a polynomial of degree q that vanishes identically on all of $\mathbb{F}_q$. Hence it is uniquely determined as $x^q - x$.

Therefore,

$$\begin{aligned} \begin{bmatrix} n \\ m \end{bmatrix} &\equiv [x^m](x)^{(n)} \equiv [x^m](x)^{(n_0)}(x^q - x)^{n_1} \\ &\equiv [x^{m-n_1}](x)^{(n_0)}(x^{q-1} - 1)^{n_1} \\ &\equiv [x^{m_1(q-1)+m_0}](x)^{(n_0)}(x^{q-1} - 1)^{n_1} \pmod q. \end{aligned}$$

Now since $(x)^{(n_0)}$ is a polynomial of degree n_0 and $(x^{q-1}-1)^{n_1}$ is a polynomial in x^{q-1}, no additions of terms of the form $x^{i(q-1)}(x)^{(n_0)}$ can occur unless $n_0 = q-1$, and in this case would become only relevant for $m_0 = 0$.

We conclude the proof by treating this two cases.

- $n_0 \neq q-1$ or $n_0 = q-1$, $m_0 \neq 0$:

$$\begin{aligned} a^{n-m}\begin{bmatrix} n \\ m \end{bmatrix} &\equiv a^{n_0-m_0}[x^{m_1(q-1)+m_0}](x)^{(n_0)}(x^{q-1}-1)^{n_1} \\ &\equiv a^{n_0-m_0}\begin{bmatrix} n_0 \\ m_0 \end{bmatrix}\binom{n_1}{m_1}(-1)^{n_1-m_1} \pmod q. \end{aligned}$$

- $n_0 = q-1, m_0 = 0$:

$$\begin{aligned} a^{n-m}\begin{bmatrix} n \\ m \end{bmatrix} &\equiv a^{n_0-m_0}[x^{m_1(q-1)+m_0}](x)^{(n_0)}(x^{q-1}-1)^{n_1} \\ &\equiv a^{n_0-m_0}\begin{bmatrix} n_0 \\ 0 \end{bmatrix}\binom{n_1}{m_1}(-1)^{n_1-m_1} \\ &\quad + a^{n_0-m_0}\begin{bmatrix} n_0 \\ q-1 \end{bmatrix}\binom{n_1}{m_1-1}(-1)^{n_1-(m_1-1)} \pmod q, \end{aligned}$$

but the first term vanishes by $\left[\begin{smallmatrix} q-1 \\ 0 \end{smallmatrix}\right] = 0$ and thus the assertion follows. □

Example 3. *For the special case $q = 2$ the formula reduces considerably. Let $n = n_0 + 2n_1$, $0 \leq n_0 < 2$, then*

$$\begin{bmatrix} n \\ m \end{bmatrix} \equiv \binom{n_1}{m-n_1-n_0} = \binom{\lfloor n/2 \rfloor}{m - \lfloor (n+1)/2 \rfloor} \pmod 2.$$

(This corresponds to Example 3 in [6]*)*

Now we can state how our finite-row generator matrices are built up from $q \times q$ submatrices in a similar manner as the Pascal matrices. The special structure of $Q(a)$ is important here.

Theorem 3. *Let the matrix given by $S_1(a)Q(a)^l$ with $a \neq 0, l \in \{0, 1, \ldots, q-1\}$ be denoted by $C(a, l) = (c(a, l)_{k,j})_{k,j \geq 1}$. The following holds true for all $k, j \in \mathbb{N}$*

$$c(a,l)_{k,j} \quad \equiv \quad c(a,l)_{k_0,j_0} p^{(q-1)}_{k_1+1,j_1+1} + \delta_{1,k_0} c(a,l)_{q,j_0} p^{(q-1)}_{k_1,j_1+1} \pmod q,$$

where

$$\begin{aligned} j = j_1 q + j_0, &\quad 0 < j_0 \leq q, \\ k - j_1 = k_1(q-1) + k_0, &\quad 0 < k_0 \leq q-1. \end{aligned}$$

Proof. First we rewrite the formula of Proposition 3 as

$$\begin{aligned} a^{n-m}\begin{bmatrix} n \\ m \end{bmatrix} \quad \equiv \quad & a^{n_0-m_0}\begin{bmatrix} n_0 \\ m_0 \end{bmatrix}(-1)^{n_1-m_1}\binom{n_1}{m_1} \\ & + \delta_{0,m_0} a^{n_0-(q-1)}\begin{bmatrix} n_0 \\ q-1 \end{bmatrix}(-1)^{n_1-(m_1-1)}\binom{n_1}{m_1-1} \pmod q. \end{aligned}$$

Note that whenever $m_0 \neq 0$ or $n_0 \neq q-1$ the second term vanishes since $\delta_{0,m_0} = 0$ or $\begin{bmatrix} n_0 \\ q-1 \end{bmatrix} = 0$ and if $m_0 = 0$ and $n_0 = q-1$ then the first term vanishes since $\begin{bmatrix} q-1 \\ 0 \end{bmatrix} = 0$.

From this it is easy to derive the formula above in the case where $b = 0$. We just have to take care about the indices and use that $(-1)^{n_1-m_1}\binom{n_1}{m_1} = p^{(q-1)}_{m_1+1,n_1+1}$:

$$c(a,0)_{k,j} \equiv c(a,0)_{k_0,j_0} p^{(q-1)}_{k_1+1,j_1+1} + \delta_{1,k_0} c(a,0)_{q,j_0} p^{(q-1)}_{k_1,j_1+1} \pmod q. \quad (2)$$

We recall the special structure of $Q(a)$ given in the proof of Corollary 1:

$$Q(a) = \begin{pmatrix} B & 0 & 0 & \cdots \\ 0 & B & 0 & \cdots \\ \vdots & 0 & \ddots & \cdots \\ \vdots & \vdots & \ddots & \ddots \end{pmatrix}$$

with

$$B = \begin{pmatrix} 1 & (q-1)a & 0 & \cdots & \cdots \\ 0 & 1 & (q-2)a & 0 & \cdots \\ \vdots & 0 & \ddots & \ddots & \ddots \\ \vdots & \vdots & 0 & 1 & a \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} \in \mathbb{F}_q{}^{q\times q}.$$

Now we do not think about the effect of $Q(a)$ on the digit vector as in the proof of Corollary 1 but on the effect on the matrix C that is multiplied. We compute the columns of $C \cdot Q(a)$ by applying the special structure of B:
For the first column we just take the first column of C. For the second column we multiply the first column of C with $(q-1)a$ and add it to the second column of C. And so on. For the qth column we multiply the $(q-1)$th column of C with a and add it to the qth column of C. Now for the $(q+1)$th column we just take the $(q+1)$th column of C. It should be clear how to go on. Altogether we see that the multiplication of any matrix with $Q(a)$ from the right brings an operation on the jth column that is uniquely determined by j_0 and combines the columns only local in the range of $j \in \{qj_1 + r : 1 \leq r \leq q\}$.

More exactly we get for the entries of $C(a,l) = C(a,l-1)Q(a) = C(a,0)Q(a)^l$ that

$$\begin{aligned} c(a,l)_{k,j} &\equiv c(a,l)_{k,j_1q+j_0} \\ &\equiv c(a,l-1)_{k,j_1q+j_0} + (q-j_0+1)ac(a,l-1)_{k,j_1q+j_0-1} \end{aligned}$$

$$\equiv \sum_{n=0}^{\min\{l,j_0-1\}} c(a,0)_{k,j_1q+j_0-n}(-a)^n \binom{l}{n}(j_0-1)_n \pmod{q}.$$

For the latter compare the proof of Theorem 2 and note that $q|(j_0-1)_n$ whenever $n \geq j_0$. From the restriction on n we get that $1 \leq j_0 - n \leq j_0 \leq q$ and we can use (2) for

$$c(a,0)_{k,j_1q+j_0-n} \equiv c(a,0)_{k_0,j_0-n}p^{(q-1)}_{k_1+1,j_1+1} + \delta_{1,k_0}c(a,0)_{q,j_0-n}p^{(q-1)}_{k_1,j_1+1} \pmod{q}.$$

We obtain

$$\begin{aligned} c(a,l)_{k,j} \equiv{} & p^{(q-1)}_{k_1+1,j_1+1} \sum_{n=0}^{\min\{l,j_0-1\}} c(a,0)_{k_0,j_0-n}(-a)^n \binom{l}{n}(j_0-1)_n \\ & + p^{(q-1)}_{k_1,j_1+1}\delta_{1,k_0} \sum_{n=0}^{\min\{l,j_0-1\}} c(a,0)_{q,j_0-n}(-a)^n \binom{l}{n}(j_0-1)_n \pmod{q}. \end{aligned}$$

Finally we use

$$\sum_{n=0}^{\min\{l,j_0-1\}} c(a,0)_{k_0,j_0-n}(-a)^n \binom{l}{n}(j_0-1)_n = c(a,l)_{k_0,j_0}$$

and

$$\sum_{n=0}^{\min\{l,j_0-1\}} c(a,0)_{q,j_0-n}(-a)^n \binom{l}{n}(j_0-1)_n = c(a,l)_{q,j_0}$$

and the result follows. □

Note that for $j_0 = q$, $k_0 = 1$ and $l = q-1$ we get

$$\begin{aligned} c(a,q-1)_{1,q} &\equiv \sum_{n=0}^{q-1} c(a,0)_{1,q-n}(-a)^n \binom{q-1}{n}(q-1)_n \\ &\equiv c(a,0)_{1,1}(q-1)! \equiv q-1 \pmod{q} \end{aligned}$$

and

$$\begin{aligned} c(a,q-1)_{q,q} &\equiv \sum_{n=0}^{q-1} c(a,0)_{q,q-n}(-a)^n \binom{q-1}{n}(q-1)_n \\ &\equiv c(a,0)_{q,q} \equiv 1 \pmod{q}. \end{aligned}$$

Hence both terms are not zero in that case and we cannot simplify the formula as in Proposition 3. This overlapping of the self-similar structure can be checked in the 4th matrix in Figure 2, see e.g. the 10th entry in the 6th row.

The assertion of the preceding theorem can be visualized as follows. To construct $S_1(a) = Q(a)^l = C(a,l)$ for any $l \in \{0,1,\ldots,q-1\}$ we compute its upper left $(q \times q)$ submatrix. Then we use this submatrix as unit and apply the construction principle of $P^{(q-1)}$ to build up $(qi \times qi)$ matrices. Finally the $(q \times q)$ units are shifted down s rows, where $s = j_1 - k_1$, and overlapping parts of the units are added in $\mathbb{F}_q$.

3. Remarks and Open Questions

The next interesting question is of course how to generalize the results in this paper to Faure sequences over the general finite field $\mathbb{F}_{q^w}$ with q^w elements where $q \in \mathbb{P}$ and $w \in \mathbb{N}$. Here for an element $b \in \mathbb{F}_{q^w}$ the bth Pascal matrix over $\mathbb{F}_{q^w}$ is defined similarly by $P(b) := (p(b)_{k,j})_{k,j\geq 1}$, where $p(b)_{k,j} = \binom{j-1}{k-1} b^{j-k}$, $0^0 := 1$.

Note that Definition 1 in the finite extension field case necessitates a bijection between the set of digits $\{0,1,\ldots,q^w-1\}$ and $\mathbb{F}_{q^w}$ with the requirement that 0 maps to 0. (See e.g. [13] for more details.)

It is easy to check that for any $b_1, b_2 \in \mathbb{F}_{q^w}$ we have $P(b_1) \cdot P(b_2) = P(b_1 + b_2)$ (compare e.g. proof of Proposition 2 in [6]).

Since Proposition 1 holds also for generator matrices over general finite fields it is clear that proper scrambling matrices exist that yield finite-row generator matrices.

One approach to generalize the results in this paper would be to choose any $a \in \mathbb{F}_{q^w}, a \neq 0$ and consider the $(0,q)$-sequence generated by $P(a), P(a + a), \cdots, P(q \cdot a = 0)$. Then the matrix $S(a) := (\left[\begin{smallmatrix} j-1 \\ k-1 \end{smallmatrix} \right] a^{j-k})_{k,j\geq 1}$ yields corresponding results over the finite field. But nevertheless if $w > 1$ we don't exhaust the full dimension q^w that should be possible.

This yields the following interesting open problem.

Open Problem 1. *Find an explicit formula for a scrambling matrix that modifies the q^w Pascal matrices over the finite field with q^w elements to proper generator matrices with shortest possible row lengths of a finite-row digital $(0, q^w)$-sequence.*

Niederreiter [12] introduced the digital (t,s)-sequences over $\mathbb{F}_{q^w}$ where the generator matrices are determined by the coefficients of the formal Laurent series of certain rational functions over the finite field $\mathbb{F}_{q^w}$. This class of sequences contains the generalized Faure sequences as special cases.

Open Problem 2. *For every digital (t, s)-sequence state a proper NUT matrix which modifies the digital (t, s)-sequence to a finite-row (t, s)-sequence.*

Since the investigation of the finite-row (t, s)-sequences is motivated in the context of low-discrepancy Niederreiter-Halton sequences we are also interested in discrepancy estimates of sequences that are composed by finite-row (t, s)-sequences. For example we are interested in ...

Open Problem 3. *... good lower and upper bound for the discrepancy of the 5-dimensional Niederreiter-Halton sequence where the first two components are generated by $S_1(1), S_1(1)Q(1)$ over $\mathbb{F}_2$ and the last three components are generated by $S_1(1), S_1(1)Q(1), S_1(1)Q(1)^2$ over $\mathbb{F}_3$.*

REFERENCES

[1] J. Dick, F. Pillichshammer. Digital Nets and Sequences. Cambridge University Press. Cambridge, 2010.

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

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

[4] H. Faure, S. Tezuka, *Another Random Scrambling of Digital (t, s)-Sequences*, in: K.T. Fang, F.J. Hickernell, H. Niederreiter (Eds.), Monte Carlo and Quasi-Monte Carlo Methods 2000, Springer, Berlin, 2002, pp. 242-256.

[5] J.H. Halton. *On the efficiency of certain quasi-random sequences of points in evaluating multi-dimensional integrals*. Numer. Math. **74** (1960), no. 2, 84–90.

[6] R. Hofer, G. Larcher, *On existence and discrepancy of certain digital Niederreiter-Halton sequences*. Acta Arith. **141** (2010), no. 4, 369–394.

[7] D.E. Knuth. The art of computer programming. Volume 1: Fundamental algorithms. Second printing of the Second edition. Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1975.

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

[9] G. Larcher, 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] C. Lemieux. Monte Carlo and Quasi-Monte Carlo Sampling. Springer Series in Statistics. Springer, New York, 2009.

[11] H. Niederreiter, *Point sets and sequences with small discrepancy*. Monatsh. Math. **104** (1987), 273–337.

[12] H. Niederreiter, *Low-discrepancy and low-dispersion sequences*, J. Number Theory **30** (1988), 51–70.

[13] H. Niederreiter. Random Number Generation and Quasi-Monte Carlo Methods. No. 63 in CBMS-NSF Series in Applied Mathematics. SIAM, Philadelphia, 1992.

[14] I.M. Sobol, *On the distribution of points in a cube and the approximation evaluation of integrals*, U.S.S.R. Comput. Math. Math. Phys. **7** (1967), 86–112.

[15] C. Xing and H. Niederreiter, *A construction of low-discrepancy sequences using global function fields*, Acta Arith. **LXXIII.1** (1995), 87–102.

Received January 20, 2011
Accepted April 7, 2011

Institut für Finanzmathematik, Universität Linz,
Altenbergerstraße 69, A-4040 Linz, Austria
E-mail: roswitha.hofer@jku.at and gpirsic@gmail.com