Constructions and properties of finite-row (t, s)-sequences[1]

Roswitha Hofer[2]

Institute of Financial Mathematics, University of Linz, Austria

June 2012, UDT12, Smolenice, Slovakia

[1] Partially joint work with Pirsic and with Larcher

[2] supported by the Austrian Science Fund (FWF), Project P21943.

Topics of the talk

- Definition of (finite-row) digital (t, s)-sequences
- Constructions/Examples of (finite-row) digital (t, s)-sequences
- Some specific properties

Definition (digital sequence over $\mathbb{F}_q$ by Niederreiter 1987)

s ...dimension, $\mathbb{F}_q$... a finite field, $\pi : \{0, 1, \dots, q-1\} \to \mathbb{F}_q$ ... a bijection, $C_1, \dots, C_s$ ... $(\infty \times \infty)$-matrices over $\mathbb{F}_q$, .

$x_n^{(i)}$ of the sequence $\left((x_n^{(1)}, \dots, x_n^{(s)})\right)_{n \geq 0} \in [0,1)^s$ is generated as follows.

Let $n = n_0 + n_1 q + n_2 q^2 + \cdots$ with $n_j \in \{0, 1, \dots, q-1\}$. Compute

$$C_i \cdot \begin{pmatrix} \pi(n_0) \\ \pi(n_1) \\ \vdots \end{pmatrix} = \begin{pmatrix} y_0^{(i)} \\ y_1^{(i)} \\ \vdots \end{pmatrix} \in \mathbb{F}_q^\infty$$

and set

$$x_n^{(i)} := \frac{\pi^{-1}(y_0^{(i)})}{q} + \frac{\pi^{-1}(y_1^{(i)})}{q^2} + \frac{\pi^{-1}(y_2^{(i)})}{q^3} + \cdots .$$

- **digital** (t,s)**-sequences** ... good distribution properties! Here the generating matrices fulfill for all $m > t$ and all $d_1 + \cdots + d_s = m - t$, $(d_i \geq 0)$ that

$$C_1 = \left(\overbrace{\qquad\qquad}^{m} \}d_1 \qquad \right), \ldots, C_s = \left(\overbrace{\qquad\qquad}^{m} \}d_s \qquad \right)$$

the matrix $\overbrace{\qquad\qquad\qquad}^{m}$ $\begin{matrix} \} & d_1 \\ \vdots & \\ \} & d_s \end{matrix}$ has rank $m - t$

- **digital (t,s)-sequences** ... good distribution properties!
  Here the generating matrices fulfill for all $m > t$ and all $d_1 + \cdots + d_s = m - t$, $(d_i \geq 0)$ that

$$C_1 = \begin{pmatrix} \overbrace{\quad\quad\quad}^{m} \}d_1 & \\ & \end{pmatrix}, \ldots, C_s = \begin{pmatrix} \overbrace{\quad\quad\quad}^{m} \}d_s & \\ & \end{pmatrix}$$

the matrix $\overbrace{\quad\quad\quad\quad}^{m} \begin{matrix} \} & d_1 \\ \vdots & \\ \} & d_s \end{matrix}$ has rank $m - t$

- **finite-row (digital) sequence** ... interesting, e.g., for fast computation.
  Here the generating matrices satisfy that each **row** contains just **finitely many nonzero entries.**

Example (van der Corput sequence = finite-row $(0,1)$-sequence)

The van der Corput sequence in base q is a digital $(0,1)$-sequence, since for the generating matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & \dots \\ 0 & 1 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \in \mathbb{F}_q^{\infty \times \infty}$$

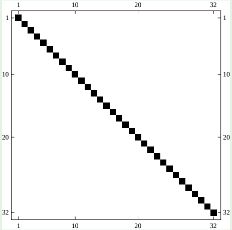
we have (1) has rank 1, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ has rank 2, $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ has rank 3, ...

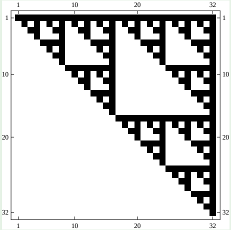
Example (digital $(0, p)$-sequences by Faure 1982)

For prime base p, the Pascal matrices $P(a)$ defined by

$$P(a) := \begin{pmatrix} 1 & \binom{1}{0}(-a)^1 & \binom{2}{0}(-a)^2 & \binom{3}{0}(-a)^3 & \dots \\ 0 & 1 & \binom{2}{1}(-a)^1 & \binom{3}{1}(-a)^2 & \dots \\ 0 & 0 & 1 & \binom{3}{2}(-a)^1 & \dots \\ \vdots & \vdots & \vdots & \ddots & \vdots \end{pmatrix} \in \mathbb{F}_p^{\infty \times \infty},$$

$a \in \{0, 1 \dots, p-1\}$ generate a digital $(0, p)$-sequence over $\mathbb{F}_p$.
For $p = 2$ (Sobol 1967) the matrices are sketched:





Example (classical Niederreiter sequences, 1988)

Take s **distinct irreducible polynomials** $h_1, h_2, \ldots, h_s$ in $\mathbb{F}_q[x]$ of degrees $e_1, e_2, \ldots, e_s$.

Now the j-th **row** of the i-th generating matrix, $(c_{j,r}^{(i)})_{r\geq 0}$, is determined using the coefficients of the formal **Laurent-series of the rational function**

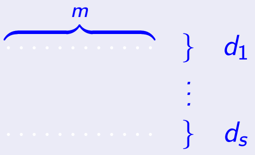
$$\frac{x^k}{(h_i(x))^l} = \sum_{r=0}^{\infty} c_{j,r}^{(i)} x^{-r-1},$$

where $0 \leq k < e_i, l \geq 1$ satisfy $j + 1 = e_i l - k$.
Then

$$t = \sum_{i=1}^{s} (e_i - 1).$$

Research Question

Let $s > 1$. *Can finite rows satisfy for all* $m > t$ *and* $d_1, \ldots, d_s \geq 0$ *with* $d_1 + \ldots + d_s = m - t$



has rank $m - t$*?*

Do there exist multi-dimensional finite-row (t, s)-sequences?

Constructions via Faure and Tezuka Scramblings

Theorem (Faure & Tezuka 2000)

If $C_1, \dots, C_s \in \mathbb{F}_q^{\infty \times \infty}$ generate a digital (t, s)-sequence over $\mathbb{F}_q$ and M is a NUT matrix over $\mathbb{F}_q$.
Then the matrices $C_1 M, \dots, C_s M$ generate a digital (t, s)-sequence.

Idea (Construct a proper "scrambling" matrix, H.& Larcher 2010)

$$\begin{pmatrix} 1 & 0 & 0 & 0 & \dots \\ 0 & 1 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \cdot \begin{pmatrix} 1 & x & x & x & x & x & \dots \\ 0 & 1 & x & x & x & x & \dots \\ 0 & 0 & 1 & x & x & x & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} = \begin{pmatrix} x & 0 & 0 & 0 & 0 & 0 & \dots \\ x & x & x & 0 & 0 & 0 & \dots \\ x & x & x & x & x & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \dots \\ 0 & 1 & 0 & 1 & \dots \\ 0 & 0 & 1 & 1 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \cdot \begin{pmatrix} 1 & x & x & x & x & x & \dots \\ 0 & 1 & x & x & x & x & \dots \\ 0 & 0 & 1 & x & x & x & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} = \begin{pmatrix} x & x & 0 & 0 & 0 & 0 & \dots \\ x & x & x & x & 0 & 0 & \dots \\ x & x & x & x & x & x & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Constructions via Faure and Tezuka Scramblings

Theorem (Faure & Tezuka 2000)

If $C_1, \dots, C_s \in \mathbb{F}_q^{\infty \times \infty}$ generate a digital (t,s)-sequence over $\mathbb{F}_q$ and M is a NUT matrix over $\mathbb{F}_q$.
Then the matrices $C_1 M, \dots, C_s M$ generate a digital (t,s)-sequence.

Idea (Construct a proper "scrambling" matrix, H.& Larcher 2010)

$$\begin{pmatrix} 1 & 0 & 0 & 0 & \cdots \\ 0 & 1 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 0 & \cdots \\ 0 & 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 1 & 1 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 1 & 1 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} = \begin{pmatrix} x & 0 & 0 & 0 & 0 & 0 & \cdots \\ x & x & x & 0 & 0 & 0 & \cdots \\ x & x & x & x & x & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots \\ 0 & 1 & 0 & 1 & \cdots \\ 0 & 0 & 1 & 1 & \cdots \\ 0 & 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 1 & 1 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 1 & 1 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} = \begin{pmatrix} x & x & 0 & 0 & 0 & 0 & \cdots \\ x & x & x & x & 0 & 0 & \cdots \\ x & x & x & x & x & x & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Constructions via Faure and Tezuka Scramblings

Theorem (Faure & Tezuka 2000)

If $C_1, \ldots, C_s \in \mathbb{F}_q^{\infty\times\infty}$ generate a digital (t,s)-sequence over $\mathbb{F}_q$ and M is a NUT matrix over $\mathbb{F}_q$.
Then the matrices $C_1 M, \ldots, C_s M$ generate a digital (t,s)-sequence.

Idea (Construct a proper "scrambling" matrix, H.& Larcher 2010)

$$\begin{pmatrix}1&0&0&0&\cdots\\0&1&0&0&\cdots\\0&0&1&0&\cdots\\0&0&0&1&\cdots\\\vdots&\vdots&\vdots&\vdots&\ddots\end{pmatrix}\cdot\begin{pmatrix}1&0&0&0&0&0&\cdots\\0&1&1&0&0&0&\cdots\\0&0&1&1&1&0&\cdots\\\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\ddots\end{pmatrix}=\begin{pmatrix}1&0&0&0&0&0&\cdots\\0&1&1&0&0&0&\cdots\\0&0&1&1&1&0&\cdots\\\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\ddots\end{pmatrix}$$

$$\begin{pmatrix}1&1&1&1&\cdots\\0&1&0&1&\cdots\\0&0&1&1&\cdots\\0&0&0&1&\cdots\\\vdots&\vdots&\vdots&\vdots&\ddots\end{pmatrix}\cdot\begin{pmatrix}1&0&0&0&0&0&\cdots\\0&1&1&0&0&0&\cdots\\0&0&1&1&1&0&\cdots\\\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\ddots\end{pmatrix}=\begin{pmatrix}1&1&0&0&0&0&\cdots\\0&1&1&1&0&0&\cdots\\0&0&1&0&1&1&\cdots\\\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\ddots\end{pmatrix}$$

- We see: one can compute for given generating matrices of a digital (t, s)-sequence a proper scrambling NUT matrix that yields finite rows in the resulting matrices ...
- BUT a lot of computation must be done ...
- Maybe we can find explicit formulas for some examples ...

- We see: one can compute for given generating matrices of a digital (t, s)-sequence a proper scrambling NUT matrix that yields finite rows in the resulting matrices ...
- BUT a lot of computation must be done ...
- Maybe we can find explicit formulas for some examples ...

Figure: The Pascal matrices in base 2 and the modified finite-row matrices.

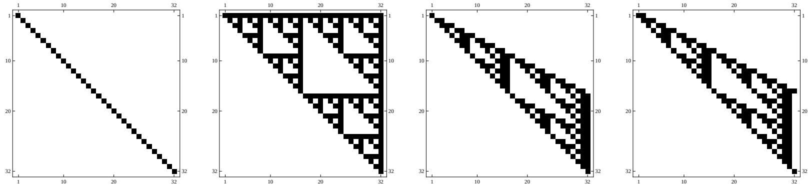


Figure: The Pascal matrices in base 5:

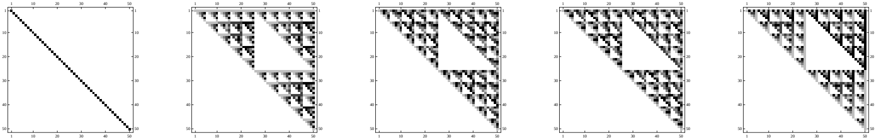
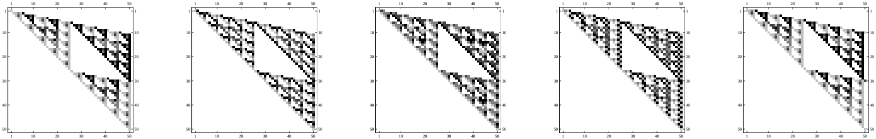


Figure: The scrambled matrices in base 5:



A formula for the scrambling matrix?

- We have a **formula for a scrambling matrix** that can be used for the generating matrices of the **Faure sequences**.
  .... (H. & Pirsic 2011)

- We also have a **formula for a scrambling matrix** that can be used for the generating matrices of the **classical Niederreiter sequences**.
  .... (H. & Pirsic 2012)

Interesting properties:

Faure sequences over $\mathbb{F}_p$ is generated by $P(0), P(1), \dots, P(p-1)$ with

$$P(a) = \left(\binom{r}{j}(-a)^{r-j}\right)_{j\geq 0, r\geq 0} \pmod{p}.$$

- A scrambling matrix that yields finite rows is

$$S = \left(\begin{bmatrix} r \\ j \end{bmatrix}\right)_{j\geq 0, r\geq 0} \pmod{p},$$

  where $\begin{bmatrix} r \\ j \end{bmatrix}$ denotes the Stirling numbers of the first kind.
- Furthermore the new generating matrices satisfy

$$P(a)S = SQ^a$$

Interesting properties:

Faure sequences over $\mathbb{F}_p$ is generated by $P(0), P(1), \ldots, P(p-1)$ with

$$P(a) = \left(\binom{r}{j}(-a)^{r-j}\right)_{j\geq 0, r\geq 0} \pmod p.$$

- A scrambling matrix that yields finite rows is

$$S = \left(\begin{bmatrix} r \\ j \end{bmatrix}\right)_{j\geq 0, r\geq 0} \pmod p,$$

  where $\begin{bmatrix} r \\ j \end{bmatrix}$ denotes the Stirling numbers of the first kind.
- Furthermore the new generating matrices satisfy

$$P(a)S = SQ^a \text{ or } S^{-1}P(a)S = Q^a \text{ with } Q = \begin{pmatrix} 1 & -1 & 0 & 0 & 0 & \cdots \\ 0 & 1 & -2 & 0 & 0 & \cdots \\ 0 & 0 & 1 & -3 & 0 & \cdots \\ \vdots & \ddots & \ddots & \ddots & \ldots & \end{pmatrix}.$$

... **Scrambling to finite-rows** here is related to **simultaneous almost diagonalization.**

Column-wise construction, H. 2012

Take s **distinct monic irreducible polynomials** $h_1, \ldots, h_s$ in $\mathbb{F}_q[x]$ of degrees $e_1, \ldots, e_s$ and
a sequence $(p_r)_{r \geq 0}$ in $\mathbb{F}_q[x]$ satisfying $\deg(p_r) = r$.

Now the r-**th column** of the i-**th generating matrix** is determined

Column-wise construction, H. 2012

Take s **distinct monic irreducible polynomials** $h_1, \ldots, h_s$ in $\mathbb{F}_q[x]$ of degrees $e_1, \ldots, e_s$ and
a sequence $(p_r)_{r\geq 0}$ in $\mathbb{F}_q[x]$ satisfying $\deg(p_r) = r$.

Now the r-**th column** of the i-**th generating matrix** is determined using the **representation of** $p_r(x)$ **in terms of powers of** $h_i(x)$:

$$p_r(x) = \rho_0(x) + \rho_1(x)h_i(x) + \rho_2(x)h_i(x)^2 + \cdots = \sum_{k=0}^{\infty} \rho_k(x)h_i(x)^k$$

where the $\rho_k(x)$ have degrees $< e_i$. Now...
- the coefficients of $\rho_0(x)$ determine the first e_i entries of the column,
- the coefficients of $\rho_1(x)$ determine the next e_i entries of the column,
- ...

This construction yields

$$t = \sum_{i=1}^{s} (e_i - 1).$$

Example (Faure sequence over $\mathbb{F}_p$)

- $h_1(x) = x, h_2(x) = x + 1, \ldots, h_p(x) = x + (p - 1)$ and
- $p_r(x) = x^r$.

Using the binomial theorem we see:

$$x^r = (x + a - a)^r = \sum_{k=0}^{r} \binom{r}{k} (-a)^{r-k} (x + a)^k.$$

Matrix entries are given by such terms

$$c_{j,r}(a) = \binom{r}{j} (-a)^{r-j}.$$

Example (Finite-row $(0, p)$-sequences over $\mathbb{F}_p$)

- $h_1(x) = x, h_2(x) = x + 1, \ldots, h_p(x) = x + (p - 1)$ and
- $p_r(x) = x(x + 1) \cdots (x + r - 1) = (x)^{(r)}$...**rising factorial** modulo p.

(I) We see that for r big enough $(x)^{(r)}$ can be divided by $(x + a)$ with residue 0 several times! THIS YIELDS FINITE ROWS.

Example (Finite-row $(0, p)$-sequences over $\mathbb{F}_p$)

- $h_1(x) = x, h_2(x) = x + 1, \ldots, h_p(x) = x + (p-1)$ and
- $p_r(x) = x(x+1)\cdots(x+r-1) = (x)^{(r)}$...**rising factorial** modulo p.

(II) Furthermore, the rising factorials are related to the Stirling numbers as follows:

$$x(x+1)(x+2)\cdots(x+r-1) = \sum_{k=0}^{r} \begin{bmatrix} r \\ k \end{bmatrix} x^k.$$

The matrix related to $h_1(x) = x$ is

$$S = \left(\begin{bmatrix} r \\ j \end{bmatrix} \right)_{j \geq 0, r \geq 0} \pmod{p}.$$

Example (Finite-row $(0, p)$-sequences over $\mathbb{F}_p$)

- $h_1(x) = x, h_2(x) = x + 1, \ldots, h_p(x) = x + (p - 1)$ and
- $p_r(x) = x(x + 1) \cdots (x + r - 1) = (x)^{(r)}$...**rising factorial** modulo p.

(III) Using that

$$(x + a)^{(r)} = \sum_{k=0}^{r} \binom{r}{k} (a)^{(r-k)} (x)^{(k)},$$

one can see the relations between the generating matrices:

$$S, SQ, \ldots, SQ^{p-1} \text{ with } Q = \begin{pmatrix} 1 & -1 & 0 & 0 & 0 & \cdots \\ 0 & 1 & -2 & 0 & 0 & \cdots \\ 0 & 0 & 1 & -3 & 0 & \cdots \\ \vdots & \ddots & \ddots & \ddots & \ldots & \end{pmatrix}.$$

References:

- Faure H. Discrépance de suites associées à un système de numération (en dimension s), Acta Arith. 41 , 337–351, 1982.
- Faure H. and Tezuka S. 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.
- Hofer R. A construction of low-discrepancy sequences involving finite-row digital (t, s)-sequences. Submitted.
- Hofer R. and Larcher G. On existence and discrepancy of certain Niederreiter-Halton sequences. Acta Arith. 141, 369–394, 2010.
- Hofer R. and Pirsic G. An explicit construction of finite-row digital $(0, s)$-sequences. Uniform Distribution Theory 6, 11-28, 2011.
- Hofer R. and Pirsic G. On existence of finite-row digital (t, s)-sequences. Submitted.
- Niederreiter H. Point sets and sequences with small discrepancy. Monatsh. Math. 104 (1987), no. 4, 273–337.
- Sobol' I.M. On the distribution of points in a cube and approximate evaluation of integrals. Ž. Vyčisl. Mat. i Mat. Fiz. 7 (1967), 784-802.