A construction of \((t, s)\)-sequences with finite-row generating matrices using global function fields

Roswitha Hofer and Harald Niederreiter

May 10, 2014

Abstract

For any prime power \(q\) and any dimension \(s \geq 1\), we present a construction of \((t, s)\)-sequences in base \(q\) with finite-row generating matrices such that, for fixed \(q\), the quality parameter \(t\) is asymptotically optimal as a function of \(s\) as \(s \to \infty\). This is the first construction of \((t, s)\)-sequences that yields finite-row generating matrices and asymptotically optimal quality parameters at the same time. The construction is based on global function fields. We put the construction into the framework of \((u, e, s)\)-sequences that was recently introduced by Tezuka. In this way we obtain in many cases better discrepancy bounds for the constructed sequences than by previous methods for bounding the discrepancy.

1 Introduction and basic definitions

Constructing sequences with good equidistribution properties is an important problem in number theory and has applications to quasi-Monte Carlo methods in numerical analysis (see, e.g., [3, 16]). In this context, the star discrepancy appears as an important measure of uniform distribution. For a given dimension \(s \geq 1\), let \(J\) be a subinterval of \([0, 1]^s\) and let \(x_0, \ldots, x_{N-1}\) be \(N\) points in \([0, 1]^s\) (we speak also of a point set \(\mathcal{P}\) of \(N\) points in \([0, 1]^s\)). We write \(A(J; \mathcal{P}) = A(J; x_0, \ldots, x_{N-1})\) for the number of integers \(0 \leq n \leq N - 1\) for which \(x_n \in J\). Then the star discrepancy of the point set \(\mathcal{P}\) consisting of the points \(x_0, \ldots, x_{N-1}\) is defined by

\[
D_N^*(\mathcal{P}) = D_N^*(x_0, \ldots, x_{N-1}) = \sup_J \left| \frac{A(J; \mathcal{P})}{N} - \text{Vol}(J) \right|
\]
where the supremum is extended over all subintervals $J$ of $[0,1]^s$ with one vertex at the origin. For a sequence $S$ of points $x_0, x_1, \ldots$ in $[0,1]^s$, the star discrepancy of the first $N$ terms of $S$ is defined as $D^*_N(S) = D^*_N(x_0, \ldots, x_{N-1})$. We say that $S$ is a low-discrepancy sequence if

$$D^*_N(S) = O(N^{-1}(\log N)^s)$$

for all $N \geq 2$, where the implied constant does not depend on $N$. This is conjectured to be the least possible order of magnitude in $N$ that can be obtained for the star discrepancy of a sequence of points in $[0,1]^s$.

One of the most powerful methods for constructing low-discrepancy sequences is built on the theory of $(t,s)$-sequences and $(t,m,s)$-nets which was developed by Niederreiter [13] on the basis of earlier work by Sobol’ [22] and Faure [4]. The reader is referred to, e.g., the monographs [3] and [16] for the general background on this theory. In the following, we give a short description of the basic notions. For integers $b \geq 2$ and $0 \leq t \leq m$, a $(t,m,s)$-net in base $b$ is a point set of $b^m$ points in $[0,1)^s$ such that every elementary interval $J \subseteq [0,1)^s$ in base $b$ with volume $b^{t-m}$ contains exactly $b^t$ points of the point set. By an elementary interval in base $b$ we mean an interval of the form

$$\prod_{i=1}^s [a_i b^{-d_i}, (a_i + 1)b^{-d_i})$$

with integers $d_i \geq 0$ and $0 \leq a_i < b^{d_i}$ for $1 \leq i \leq s$. A sequence $x_0, x_1, \ldots$ of points in $[0,1]^s$ is called a $(t,s)$-sequence in base $b$, where $b \geq 2$ and $t \geq 0$ are integers, if for all integers $k \geq 0$ and $m > t$ the points $[x_n]_{k,m}$ with $kb^m \leq n < (k+1)b^m$ form a $(t,m,s)$-net in base $b$. Here $[x_n]_{k,m}$ denotes the coordinatewise $m$-digit truncation in base $b$ of the point $x_n$. (For a detailed description we refer the reader to, e.g., [24], [25, Section 6.1.1], and [27, Section 2]; the important role of the truncation was emphasized again in the recent paper [6].) In this concept the integer $t$ serves as a quality parameter, and generally speaking the smaller $t$ the more uniform the distribution of the sequence.

Most of the known $(t,s)$-sequences are obtained by the so-called digital method which was developed by Niederreiter [13] and constructs a sequence as follows. Choose a dimension $s \in \mathbb{N}$, a finite field $\mathbb{F}_q$ with cardinality $q$, and put $Z_q = \{0,1,\ldots,q-1\} \subset \mathbb{Z}$. Note that $q$ must be a prime power here. Choose

(i) bijections $\psi_r : Z_q \to \mathbb{F}_q$ for all integers $r \geq 0$, satisfying $\psi_r(0) = 0$ for all sufficiently large $r$;

(ii) elements $c^{(i)}_{j,r} \in \mathbb{F}_q$ for $1 \leq i \leq s$, $j \geq 1$, and $r \geq 0$;
(iii) bijections $\lambda_{i,j} : \mathbb{F}_q \to \mathbb{Z}_q$ for $1 \leq i \leq s$ and $j \geq 1$.

For the construction of the sequence we make use of the notion of the generating matrices $C^{(i)} := (c_{j,r}^{(i)})_{j \geq 1, r \geq 0} \in \mathbb{F}_q^{N \times N_0}$ for $1 \leq i \leq s$. If these matrices $C^{(1)}, \ldots, C^{(s)}$ satisfy the property that each row of each matrix contains only finitely many nonzero entries, then we speak of finite-row generating matrices.

The $i$th coordinate $x_n^{(i)}$ of the $n$th point $x_n = (x_n^{(1)}, \ldots, x_n^{(s)})$ of the sequence is computed as follows. Given an integer $n \geq 0$, let $n = \sum_{r=0}^{\infty} z_r(n) q^r$ be the digit expansion of $n$ in base $q$, with all $z_r(n) \in \mathbb{Z}_q$ and $z_r(n) = 0$ for all sufficiently large $r$. Then for $1 \leq i \leq s$ we form the matrix-vector product over $\mathbb{F}_q$ given by

$$C^{(i)} \cdot \begin{pmatrix} \psi_0(z_0(n)) \\ \psi_1(z_1(n)) \\ \vdots \\ y_{n,1}^{(i)} \\ y_{n,2}^{(i)} \\ \vdots \end{pmatrix} =: \begin{pmatrix} y_{n,1}^{(i)} \\ y_{n,2}^{(i)} \\ \vdots \end{pmatrix}.$$ 

Finally, we put

$$x_n^{(i)} = \sum_{j=1}^{\infty} \lambda_{i,j}(y_{n,j}^{(i)}) q^{-j}.$$ 

The distribution of the sequence $x_0, x_1, \ldots$ is mainly determined by the rank structure of the generating matrices. It is well known that the digital method generates a $(t,s)$-sequence in base $q$ if for every integer $m > t$ and all nonnegative integers $d_1, \ldots, d_s$ such that $d_1 + \cdots + d_s = m - t$, the $(m-t) \times m$ matrix over $\mathbb{F}_q$ formed by the row vectors

$$(c_{j,0}^{(i)}, c_{j,1}^{(i)}, \ldots, c_{j,m-1}^{(i)}) \in \mathbb{F}_q^m$$

with $1 \leq j \leq d_i$ and $1 \leq i \leq s$ has rank $m - t$ (see [3, Section 4.4] and [16, Section 4.3]).

Standard $(t,s)$-sequences obtained by the digital method include the Sobol’ sequences [22], Faure sequences [4], Niederreiter sequences [14], generalized Niederreiter sequences [24], and Niederreiter-Xing sequences [18, 27]. Summaries of the constructions of these sequences can be found in [3, Chapter 8] and [17].

The digital method can be applied also for the construction of $(t,m,s)$-nets in base $q$. In this case, the generating matrices $C^{(1)}, \ldots, C^{(s)}$ are $m \times m$ matrices over $\mathbb{F}_q$ (see [3, Section 4.4.1]).

Tezuka [26] recently pointed out a deeper regularity in the generating matrices of the generalized Niederreiter sequences and introduced so-called $(u,m,e,s)$-nets and $(u,e,s)$-sequences. He also established a general discrepancy bound for $(u,e,s)$-sequences and in this way he improved the constants in the discrepancy bounds known for generalized Niederreiter sequences.
In this paper we fulfill several objectives. In Section 2 we give a revised version of Tezuka’s definition of \((u, m, e, s)\)-nets which allows us to determine a corresponding quality parameter \(t\) for a \((u, e, s)\)-sequence in the language of \((t, s)\)-sequences. In Section 3 we introduce a new construction principle for generating matrices of digital \((u, e, s)\)-sequences using global function fields. From the viewpoint of \((t, s)\)-sequences, these new sequences have the same quality parameter \(t\) as the Niederreiter-Xing sequences, but the construction is simpler. Moreover, a refined construction in Section 4 yields \((u, e, s)\)-sequences and \((t, s)\)-sequences with the same parameters as in Section 3 but with finite-row generating matrices. Finally, in Section 5 we discuss upper bounds on the star discrepancy for the sequences constructed in this paper.

2 A revised definition of \((u, e, s)\)-sequences

We follow up on the recent work of Tezuka [26] on nets and \((t, s)\)-sequences, but for several reasons (for instance, in order to prove Proposition 1 below) we slightly revise his approach.

**Definition 1** Let \(b \geq 2\), \(s \geq 1\), and \(0 \leq u \leq m\) be integers and let \(e = (e_1, \ldots, e_s) \in \mathbb{N}^s\) be an \(s\)-tuple of positive integers. A \((u, m, e, s)\)-net in base \(b\) is a point set \(P\) of \(b^m\) points in \([0, 1)^s\) such that \(A(J; P) = b^m \text{Vol}(J)\) for every elementary interval \(J\) in base \(b\) of the form

\[
J = \prod_{i=1}^{s} \left[a_i b^{-d_i}, (a_i + 1)b^{-d_i}\right]
\]

with integers \(d_i \geq 0, 0 \leq a_i < b^{d_i}\), and \(e_i | d_i\) for \(1 \leq i \leq s\) and with \(\text{Vol}(J) \geq b^{u-m}\).

**Remark 1** The classical concept of a \((u, m, s)\)-net in base \(b\) corresponds to the special case \(e = (1, \ldots, 1)\) in Definition 1. A simple and well-known propagation rule for nets states that a \((u, m, e, s)\)-net in base \(b\) is also a \((v, m, s)\)-net in base \(b\) for any integer \(v\) with \(u \leq v \leq m\) (see [3, Remark 4.9(2)] and [16, Remark 4.3]). It is trivial that this propagation rule is valid also for \((u, m, e, s)\)-nets in base \(b\).

**Remark 2** Tezuka [26] introduced Definition 1 but he used the condition \(\text{Vol}(J) = b^{u-m}\) instead of \(\text{Vol}(J) \geq b^{u-m}\). With this original definition, the propagation rule for \((u, m, e, s)\)-nets in base \(b\) mentioned in Remark 1 need not hold. For instance, choose \(b = s = 2\) and \(e = (2, 3) \in \mathbb{N}^2\). Furthermore, fix an integer \(m \geq 3\). Now take \(u = m - 3\). Then the only possible elementary
intervals $J \subseteq [0, 1)^2$ in base 2 in Definition 1 with $\text{Vol}(J) = 2^{-3}$ are of the form

$$J = [0, 1) \times [a_2/2^4, (a_2 + 1)/2^3].$$

Thus, the net property according to Tezuka’s original definition depends only on the second coordinates in the point set $\mathcal{P}$. Next take $u = m - 2$. Then the only possible elementary intervals $J \subseteq [0, 1)^2$ in base 2 in Definition 1 with $\text{Vol}(J) = 2^{-2}$ are of the form

$$J = [a_1/2^2, (a_1 + 1)/2^2) \times [0, 1).$$

Thus, the net property according to Tezuka’s original definition depends only on the first coordinates in $\mathcal{P}$. It is now clear that with Tezuka’s original definition, $\mathcal{P}$ can be a $(u, m, e, 2)$-net in base 2 for $u = m - 3$, but not for $u = m - 2$.

**Definition 2** Let $b \geq 2$, $s \geq 1$, and $u \geq 0$ be integers and let $e \in \mathbb{N}^s$. A sequence $x_0, x_1, \ldots$ of points in $[0, 1]^s$ is called a $(u, e, s)$-sequence in base $b$ if for all integers $k \geq 0$ and $m > u$ the points $[x_n]_{b,m}$ with $kb^m \leq n < (k+1)b^m$ form a $(u, m, e, s)$-net in base $b$.

Just like in Remark 1, it is clear that the classical concept of a $(u, s)$-sequence in base $b$ corresponds to the case $e = (1, \ldots, 1)$ in Definition 2.

**Remark 3** A further advantage of Definitions 1 and 2 is that we can drop the additional condition on $u$ and $m$ in Tezuka’s original definitions of $(u, m, e, s)$-nets and $(u, e, s)$-sequences in base $b$, namely that $m - u$ is of the form $j_1e_1 + \cdots + j_se_s$ with integers $j_1, \ldots, j_s \geq 0$, where as above $e = (e_1, \ldots, e_s)$.

**Proposition 1** Let $b \geq 2$, $s \geq 1$, and $0 \leq u \leq m$ be integers and let $e = (e_1, \ldots, e_s) \in \mathbb{N}^s$. Then any $(u, m, e, s)$-net in base $b$ is a $(t, m, s)$-net in base $b$ with

$$t = \min(u + \sum_{i=1}^s (e_i - 1), m).$$

**Proof.** Let $\mathcal{P}$ be a $(u, m, e, s)$-net in base $b$. If $u + \sum_{i=1}^s (e_i - 1) \geq m$, the statement is trivial. Now assume that $u + \sum_{i=1}^s (e_i - 1) < m$. We consider an elementary interval $J \subseteq [0, 1)^s$ in base $b$ of the form

$$J = \prod_{i=1}^s [a_i b^{-d_i}, (a_i + 1) b^{-d_i})$$
with \( \text{Vol}(J) \geq b^{l-m} \), i.e., with

\[
\sum_{i=1}^{s} d_i \leq m - t = m - u - \sum_{i=1}^{s} (e_i - 1). \tag{1}
\]

For each \( i = 1, \ldots, s \), let \( w_i \) be the unique integer with \( 0 \leq w_i \leq e_i - 1 \) such that \( d_i + w_i \) is a multiple of \( e_i \). Then

\[
[a_i b^{-d_i}, (a_i + 1)b^{-d_i}) = \bigcup_{h=1}^{b^{w_i}} ((a_i b^{w_i} + h - 1) b^{-d_i - w_i}, (a_i b^{w_i} + h) b^{-d_i - w_i})
\]

is the disjoint union of \( b^{w_i} \) one-dimensional elementary intervals in base \( b \) of length \( b^{-d_i - w_i} \). Consequently, \( J \) is the disjoint union of \( s \)-dimensional elementary intervals \( K_h, 1 \leq h \leq b^{w_1 + \cdots + w_s} =: H \), in base \( b \) with

\[
\text{Vol}(K_h) = \prod_{i=1}^{s} b^{-d_i - w_i} = b^{-\sum_{i=1}^{s} d_i - \sum_{i=1}^{s} w_i} \geq b^{-m + u + \sum_{i=1}^{s} (e_i - 1 - w_i)} \geq b^{u-m}
\]

for \( 1 \leq h \leq H \), where we used (1) and \( w_i \leq e_i - 1 \) for \( 1 \leq i \leq s \). By Definition 1 we have

\[
A(K_h; \mathcal{P}) = b^m \text{Vol}(K_h) \quad \text{for } 1 \leq h \leq H.
\]

Therefore

\[
A(J; \mathcal{P}) = \sum_{h=1}^{H} A(K_h; \mathcal{P}) = b^m \sum_{h=1}^{H} \text{Vol}(K_h) = b^m \text{Vol}(J),
\]

and so \( \mathcal{P} \) is a \((t, m, s)\)-net in base \( b \).

**Corollary 1** Let \( b \geq 2, s \geq 1, \) and \( u \geq 0 \) be integers and let \( \mathbf{e} = (e_1, \ldots, e_s) \in \mathbb{N}^s \). Then any \((u, \mathbf{e}, s)\)-sequence in base \( b \) is a \((t, s)\)-sequence in base \( b \) with

\[
t = u + \sum_{i=1}^{s} (e_i - 1).
\]

**Remark 4** Tezuka [26] has shown with his original definition of a \((u, \mathbf{e}, s)\)-sequence that a generalized Niederreiter sequence is a \((0, \mathbf{e}, s)\)-sequence in base \( q \), where \( \mathbf{e} = (e_1, \ldots, e_s) \in \mathbb{N}^s \) and \( e_i, 1 \leq i \leq s \), is the degree of the \( i \)th base polynomial over \( \mathbb{F}_q \) in the construction of generalized Niederreiter sequences. It is immediately seen from his proof that a generalized Niederreiter sequence is also a \((0, \mathbf{e}, s)\)-sequence in base \( q \) in the sense of
our Definition 2. Corollary 1 implies that it is a \((t, s)\)-sequence in base \(q\) with 
\[ t = \sum_{i=1}^{s}(e_i - 1). \] 
This gives another proof of this well-known result from [24]. Consider now the case of the Niederreiter sequences constructed in [14]. They form a subfamily of the generalized Niederreiter sequences, and so a Niederreiter sequence is also a \((0, e, s)\)-sequence in base \(q\) and a \((t, s)\)-sequence in base \(q\) with 
\[ t = \sum_{i=1}^{s}(e_i - 1). \] 
Dick and Niederreiter [2] proved that this \(t\)-value is the exact value of the quality parameter \(t\) for Niederreiter sequences, that is, for any Niederreiter sequence no smaller value of \(t\) is possible. The case of Niederreiter sequences shows therefore that the formula for \(t\) in Corollary 1 is in general best possible.

The parameter \(u\) of a \((u, m, e, s)\)-net in base \(q\) constructed by the digital method can be derived from the following result. We use the standard convention that an empty set of vectors from a vector space is linearly independent.

**Proposition 2** The matrices \(C^{(1)}, \ldots, C^{(s)} \in \mathbb{F}_q^{m \times m}\) generate a \((u, m, e, s)\)-net in base \(q\) if and only if, for any integers \(d_1, \ldots, d_s \geq 0\) with \(e_i|d_i\) for \(1 \leq i \leq s\) and \(d_1 + \cdots + d_s \leq m - u\), the collection of \(d_1 + \cdots + d_s\) vectors obtained by taking the first \(d_i\) row vectors of \(C^{(i)}\) for \(1 \leq i \leq s\) is linearly independent over \(\mathbb{F}_q\).

**Proof.** This follows by a straightforward adaptation of standard arguments that can be found in [3, Section 4.4.2] and [16, Section 4.3]. \(\square\)

Using Proposition 2, it is easy to determine the parameter \(u\) of a \((u, e, s)\)-sequence in base \(q\) obtained by the digital method.

**Proposition 3** The matrices \(C^{(1)}, \ldots, C^{(s)} \in \mathbb{F}_q^{N \times N_0}\) generate a \((u, e, s)\)-sequence in base \(q\) if and only if, for every integer \(m > u\) and all integers \(d_1, \ldots, d_s \geq 0\) with \(e_i|d_i\) for \(1 \leq i \leq s\) and \(1 \leq d_1 + \cdots + d_s \leq m - u\), the \((d_1 + \cdots + d_s) \times m\) matrix over \(\mathbb{F}_q\) formed by the row vectors 
\[ (c^{(i)}_{j,0}, c^{(i)}_{j,1}, \ldots, c^{(i)}_{j,m-1}) \in \mathbb{F}_q^m \]
with \(1 \leq j \leq d_i\) and \(1 \leq i \leq s\) has rank \(d_1 + \cdots + d_s\).

### 3 A construction of \((u, e, s)\)-sequences

So far, the only verified family of \((u, e, s)\)-sequences with \(e \neq (1, \ldots, 1)\) is that of generalized Niederreiter sequences, according to a result of Tezuka [26].
The construction of generalized Niederreiter sequences in [24], like the earlier construction of Niederreiter sequences in [14], is based on rational function fields over finite fields. In this section we present a new construction of \((u, e, s)\)-sequences using arbitrary global function fields. Recall that a global function field \(F\) is a finite extension of the rational function field \(F_q(x)\) for some finite field \(F_q\). If \(F_q\) is algebraically closed in \(F\), then \(F_q\) is called the full constant field of \(F\).

First we collect some basic facts and notation for global function fields. We refer to the monograph [23] for general background on global function fields. Let \(F\) be a global function field with full constant field \(F_q\) and genus \(g\) and let \(\mathbb{P}_F\) denote the set of all places of \(F\). We write \(\text{deg}(P)\) for the degree of a place \(P \in \mathbb{P}_F\) and \(\nu_P\) for the normalized discrete valuation corresponding to \(P\). A divisor \(D\) of \(F\) is a formal sum

\[ D = \sum_{P \in \mathbb{P}_F} n_P P \]

with \(n_P \in \mathbb{Z}\) for all \(P \in \mathbb{P}_F\) and all but finitely many \(n_P = 0\). We write also \(n_P = \nu_P(D)\). The degree \(\text{deg}(D)\) of a divisor \(D\) is defined by

\[ \text{deg}(D) = \sum_{P \in \mathbb{P}_F} n_P \text{deg}(P) = \sum_{P \in \mathbb{P}_F} \nu_P(D) \text{deg}(P). \]

We say that \(D_1 \leq D_2\) if \(\nu_P(D_1) \leq \nu_P(D_2)\) for all \(P \in \mathbb{P}_F\). The principal divisor \(\text{div}(f)\) of \(f \in F^*\) is defined by

\[ \text{div}(f) = \sum_{P \in \mathbb{P}_F} \nu_P(f) P. \]

The Riemann-Roch space

\[ \mathcal{L}(D) := \{ f \in F^* : \text{div}(f) + D \geq 0 \} \cup \{0\} \]

is a finite-dimensional vector space over \(F_q\). We write \(\ell(D)\) for the dimension of this vector space. Obviously, \(\mathcal{L}(D_1)\) is a subspace of \(\mathcal{L}(D_2)\) whenever \(D_1 \leq D_2\). The celebrated Riemann-Roch Theorem [23] Theorem 1.5.15 ensures that \(\ell(D) \geq \text{deg}(D) + 1 - g\), and equality holds whenever \(\text{deg}(D) \geq 2g - 1\) (see [23] Theorem 1.5.17). For a rational place \(P\) (i.e. \(\text{deg}(P) = 1\)), the Weierstrass Gap Theorem [23] Theorem 1.6.8 says that there are exactly \(g\) gap numbers \(1 = i_1 < \cdots < i_g \leq 2g - 1\), that is, integers \(i_j, 1 \leq j \leq g\), such that \(\ell((i_j - 1)P) = \ell((i_j - 1)P)\). Note that for integers \(n \geq 2g\) it is clear by the Riemann-Roch Theorem that \(\ell(nP) = \ell((n - 1)P) + 1\).
Finally, choosing a place $P \in \mathbb{P}_F$ with degree $e$ and a local parameter $z$ at $P$, that is, an element $z \in F$ such that $\nu_P(z) = 1$, then any $f \in F$ has a local expansion at the place $P$ of the form

$$f = \sum_{k=k_0}^{\infty} \beta_k z^k,$$

where $k_0 \in \mathbb{Z}$ with $\nu_P(f) \geq k_0$ and $\beta_k \in \mathbb{F}_{q^e}$ for all $k \geq k_0$. A detailed description of how to obtain a local expansion can be found in [20, pp. 5–6].

For our construction we choose a dimension $s \in \mathbb{N}$, a finite field $\mathbb{F}_q$, a global function field $F$ with full constant field $\mathbb{F}_q$ and genus $g$, and $s + 1$ distinct places $P_\infty, P_1, \ldots, P_s$ of $F$ satisfying $\deg(P_\infty) = 1$. The degrees of the places $P_1, \ldots, P_s$ are arbitrary and we put $e_i = \deg(P_i)$ for $1 \leq i \leq s$. First we construct a sequence $(y_r)_{r \geq 0}$ of elements of $F$ using the information on the dimensions $\ell(nP)$ for $n \in \mathbb{N}_0$ collected above. This allows us to choose for each integer $r \geq 0$ an element $y_r \in \mathcal{L}(n_r P_\infty) \setminus \mathcal{L}((n_r - 1)P_\infty)$.

Here $n_0 < n_1 < n_2 < \cdots$ are the elements in increasing order of $\mathbb{N}_0 \setminus \{i_1, \ldots, i_g\}$, where $i_1, \ldots, i_g$ are the $g$ gap numbers of $P_\infty$. Note that $n_r = r + g$ for $r \geq g$. From the construction of the $y_r$ we see that $\nu_P(y_r) \geq 0$ for all places $P \in \mathbb{P}_F \setminus \{P_\infty\}$ and all $r \geq 0$. Thus for $1 \leq i \leq s$, the local expansion of $y_r$ at $P_i$ (with local parameter $z_i$ at $P_i$) has the form

$$y_r = \sum_{k=0}^{\infty} \beta_{k,r}^{(i)} z_i^k \quad \text{with all } \beta_{k,r}^{(i)} \in \mathbb{F}_{q^{e_i}}.$$

Using an ordered basis of $\mathbb{F}_{q^{e_i}} / \mathbb{F}_q$, we can identify $\beta_{k,r}^{(i)}$ with a column vector $b_{k,r}^{(i)} \in \mathbb{F}_{q^{e_i}}$.

Now we construct generating matrices $C^{(i)}$, $1 \leq i \leq s$, over $\mathbb{F}_q$ columnwise by defining column 0, column 1, etc. For column $r$ ($r \geq 0$) of $C^{(i)}$, we concatenate the column vectors $b_{k,r}^{(i)}$, $k = 0, 1, \ldots$. This completes the construction.

**Theorem 1** Let $F$ be a global function field with full constant field $\mathbb{F}_q$ and let $P_\infty, P_1, \ldots, P_s$ be $s + 1$ distinct places of $F$ with $\deg(P_\infty) = 1$. Then the matrices $C^{(1)}, \ldots, C^{(s)} \in \mathbb{F}_q^{N \times N_0}$ constructed above generate a $(u, e, s)$-sequence in base $g$ with $u = g$ and $e = (e_1, \ldots, e_s)$, where $g$ is the genus of $F$ and $e_i = \deg(P_i)$ for $1 \leq i \leq s$. 

9
Proof. We write $C^{(i)} = \left( c_{j,r}^{(i)} \right)_{j \geq 1, r \geq 0} \in \mathbb{F}_q^{N \times N_0}$ for $1 \leq i \leq s$. According to Proposition 3, it suffices to show that for every integer $m > g$ and all $d_1, \ldots, d_s \in \mathbb{N}_0$ such that $e_i | d_1, \ldots, e_s | d_s$ and $1 \leq d_1 + \cdots + d_s \leq m - g$, the $(d_1 + \cdots + d_s) \times m$ matrix $M$ over $\mathbb{F}_q$ formed by the row vectors

$$(c_{j,0}^{(i)}, c_{j,1}^{(i)}, \ldots, c_{j,m-1}^{(i)}) \in \mathbb{F}_q^m$$

with $1 \leq j \leq d_i$ and $1 \leq i \leq s$ has rank $d_1 + \cdots + d_s$.

In order to prove this assertion, we show that the kernel of $M$ has dimension $\leq m - (d_1 + \cdots + d_s)$. We take an arbitrary element $(v_0, \ldots, v_{m-1}) \in \mathbb{F}_q^m$ of the kernel of $M$. Then

$$\sum_{r=0}^{m-1} v_r c_{j,r}^{(i)} = 0 \quad \text{for } 1 \leq j \leq d_i, \ 1 \leq i \leq s. \quad (2)$$

In the following, we make use of the element $f := \sum_{r=0}^{m-1} v_r y_r$ of $F$. From the construction of the $y_r$ and the definition of $f$ we derive that

$$f \in \mathcal{L}(n_{m-1}P_\infty),$$

which is a Riemann-Roch space over $\mathbb{F}_q$ with dimension $m$ since the divisor $n_{m-1}P_\infty = (m + g - 1)P_\infty$ has degree $m + g - 1 > 2g - 1$. Note that $y_0, \ldots, y_{m-1}$ form a basis of this Riemann-Roch space, and so each element of $\mathcal{L}(n_{m-1}P_\infty)$ has a unique representation as an $\mathbb{F}_q$-linear combination of $y_0, \ldots, y_{m-1}$.

From (2) and the construction of the matrices $C^{(1)}, \ldots, C^{(s)}$ we deduce that

$$\nu_{P_i}(f) \geq \frac{d_i}{e_i} \quad \text{for } 1 \leq i \leq s.$$ 

Therefore

$$f \in \mathcal{L} \left( n_{m-1}P_\infty - \sum_{i=1}^{s} \frac{d_i}{e_i} P_i \right),$$

which is a subspace of $\mathcal{L}(n_{m-1}P_\infty)$. The degree of the divisor

$$D := n_{m-1}P_\infty - \sum_{i=1}^{s} \frac{d_i}{e_i} P_i$$

satisfies

$$\deg(D) = m + g - 1 - (d_1 + \cdots + d_s) \geq 2g - 1.$$
By the Riemann-Roch Theorem we know that the dimension of \( \mathcal{L}(D) \) is 
\[ m - (d_1 + \cdots + d_s). \]
In view of the one-to-one correspondence between elements of \( \mathbb{F}_q^m \) and elements of \( \mathcal{L}(n_{m-1}P_\infty) \) noted above, this yields the desired upper bound on the dimension of the kernel of \( M \).

**Corollary 2** With the conditions and notation in Theorem 1, the matrices \( C^{(1)}, \ldots, C^{(s)} \) constructed above generate a \((t, s)\)-sequence in base \( q \) with quality parameter \( t = g + \sum_{i=1}^{s} (e_i - 1) \).

**Proof.** This follows immediately from Theorem 1 by applying Corollary 1. □

**Example 1** If \( F = \mathbb{F}_q(x) \) is the rational function field over \( \mathbb{F}_q \) (here \( g = 0 \)) and \( P_\infty \) is the infinite place of \( F \), then the sequence \( (y_r)_{r \geq 0} \) consists of elements of the polynomial ring \( \mathbb{F}_q[x] \) and we have \( \operatorname{deg}(y_r) = r \) for all \( r \geq 0 \). Furthermore, if \( P_1, \ldots, P_s \) are places of \( F \) corresponding to distinct monic irreducible polynomials over \( \mathbb{F}_q \) (see [23, Section 1.2]), which serve as local parameters in the local expansions, then our construction is consistent with the one introduced in [8].

**Remark 5** So far, the known constructions of generating matrices for digital \((t, s)\)-sequences using arbitrary global function fields proceeded rowwise. The rowwise approach constructs for each component \( i \in \{1, \ldots, s\} \) a sequence of elements in the global function field via Riemann-Roch spaces [18, 27] or via differentials [12]. Then the row entries of the generating matrices are determined by using the coefficients of the local expansions of these elements at a fixed rational place. Our columnwise method constructs a sequence of elements in the global function field using Riemann-Roch spaces that are built using a fixed rational place. Then the columns of the \( i \)th generating matrix \( C^{(i)} \) are determined by using the coefficients of the local expansions at the place \( P_i \) corresponding to the \( i \)th component. The first columnwise construction of generating matrices was introduced by Niederreiter [15], which was later generalized by Hofer [7, 8]. Those constructions exploited properties of certain elements of the polynomial ring \( \mathbb{F}_q[x] \).

**Remark 6** The basic ingredients of the construction of Niederreiter-Xing sequences in [27] are, as in our construction, a global function field \( F \) with full constant field \( \mathbb{F}_q \) and \( s + 1 \) distinct places \( P_\infty, P_1, \ldots, P_s \) of \( F \) with \( \operatorname{deg}(P_\infty) = 1 \) and the degrees \( e_i = \operatorname{deg}(P_i) \) for \( 1 \leq i \leq s \) being arbitrary. We claim that a Niederreiter-Xing sequence with these data is a \((g, e, s)\)-sequence in base \( q \), where \( g \) is the genus of \( F \) and \( e = (e_1, \ldots, e_s) \). This is shown by an appropriate modification of the proof of [27, Theorem 1]. We adhere to the notation in that proof. In view of Proposition 3 it suffices to show that
for every integer \( m > g \) and all \( d_1, \ldots, d_s \in \mathbb{N}_0 \) such that \( e_1 | d_1, \ldots, e_s | d_s \) and \( 1 \leq d_1 + \cdots + d_s \leq m - g \), the vectors \( \pi_m(e_j^{(i)}) \in \mathbb{F}_q^m, 1 \leq j \leq d_i, 1 \leq i \leq s \), are linearly independent over \( \mathbb{F}_q \). In the course of the proof of [27, Theorem 1], an auxiliary element

\[
k \in \mathcal{L}
\biggl(D + \sum_{i=1}^s \left( \left\lfloor \frac{d_i - 1}{e_i} \right\rfloor + 1 \right) P_i \biggr) = \mathcal{L}
\biggl(D + \sum_{i=1}^s \frac{d_i}{e_i} P_i \biggr)
\]

is considered. Furthermore, it is shown that \( \nu_{P_{\infty}}(k) \geq m + g + 1 \). These two facts, together with \( \nu_{P_{\infty}}(D) = 0 \), imply that

\[
k \in \mathcal{L}
\biggl(D + \sum_{i=1}^s \frac{d_i}{e_i} P_i - (m + g + 1) P_{\infty} \biggr).
\]

Since \( \deg(D) = 2g \), we have

\[
\deg \left(D + \sum_{i=1}^s \frac{d_i}{e_i} P_i - (m + g + 1) P_{\infty} \right) = g + \sum_{i=1}^s d_i - m - 1 < 0,
\]

and so \( k = 0 \) by [23, Corollary 1.4.12(b)]. An appeal to [27, Lemma 2] completes the proof. By Corollary [1], the Niederreiter-Xing sequence under consideration is a \((t, s)\)-sequence in base \( q \) with \( t = g + \sum_{i=1}^s (e_i - 1) \). This recovers the main result of [27] in a different way. This value of \( t \) is the same as in Corollary [2]. However, it should be pointed out that our new construction is considerably simpler than the one in [27]. For instance, the auxiliary positive divisor \( D \) of \( \mathbb{F}_q \) with \( \deg(D) = 2g \) and \( \nu_{P_{\infty}}(D) = 0 \) in [27] is not needed in our construction.

4 Finite-row generating matrices for \((u, e, s)\)-sequences

Columnwise constructions as in this paper have certain advantages, for instance, one may obtain finite-row generating matrices more easily with this approach. For more details and the motivation for finite-row generating matrices, we refer the interested reader to [7, 8] and the references therein. To drive home an important point, we cannot refrain from emphasizing one great asset of finite-row generating matrices, namely that the sparsity of finite-row generating matrices leads to a considerable speedup in the computation of the matrix-vector products that form the main operation in the actual implementation of the digital method (see Section [1]).
In this section we explore a more refined version of the columnwise construction in Section 3 using global function fields. We choose the \( y_r \) in the sequence \((y_r)_{r \geq 0}\) by using subspaces of \( \mathcal{L}(n_r, P_{\infty}) \) and in this way we are able to construct finite-row generating matrices with, in a certain sense, optimal row lengths.

As in Section 3, let \( s \in \mathbb{N} \) be a given dimension, let \( \mathbb{F}_q \) be a finite field, let \( F \) be a global function field with full constant field \( \mathbb{F}_q \) and genus \( g \), and let \( P_\infty, P_1, \ldots, P_s \) be \( s + 1 \) distinct places of \( F \) satisfying \( \deg(P_\infty) = 1 \) and \( \deg(P_i) = e_i \) for \( 1 \leq i \leq s \). We construct \((y_r)_{r \geq 0}\) as before, but in the case where \( r > g \) we choose \( y_r \) such that

\[
y_r \in \mathcal{L}
\left(n_r P_{\infty} - \sum_{i=1}^{s} (l_i + l_{i+1} + \cdots + l_s) \frac{v}{e_i} P_i\right) =: \mathcal{L}(D_r)
\]

and

\[
y_r \notin \mathcal{L}
\left(n_{r-1} P_{\infty} - \sum_{i=1}^{s} (l_i + l_{i+1} + \cdots + l_s) \frac{v}{e_i} P_i\right) =: \mathcal{L}(D'_r).
\]

Here \( v := \text{lcm}(e_1, \ldots, e_s) \), whereas the integers \( l_i \geq 0 \) are determined by division with remainder in the nonnegative integers as follows:

\[
\begin{align*}
r - g &= svl_s + w_s, \quad w_s \in \{0, \ldots, sv-1\}, \\
        w_s &= (s-1)vl_{s-1} + w_{s-1}, \quad w_{s-1} \in \{0, \ldots, (s-1)v-1\}, \\
        &\vdots \\
        w_2 &= vl_1 + w_1, \quad w_1 \in \{0, \ldots, v-1\}.
\end{align*}
\]

Note that such a \( y_r \) exists since \( D'_r \leq D_r \) and \( \deg(D_r) \geq r + g - (r - g) = 2g \) and \( \deg(D'_r) = \deg(D_r) - 1 \). The rest of the construction is carried out as in Section 3 and leads to the new generating matrices \( C^{(1)}, \ldots, C^{(s)} \in \mathbb{F}_q^{N \times N_0} \).

From the proof of Theorem 1 and from Corollary 2 we see that the generating matrices \( C^{(1)}, \ldots, C^{(s)} \) constructed in this way within the digital method yield a \((g, e, s)\)-sequence in base \( q \) with \( e = (e_1, \ldots, e_s) \) and also a \((t, s)\)-sequence in base \( q \) with \( t = g + \sum_{i=1}^{s} (e_i - 1) \). Our more refined choice of the sequence \((y_r)_{r \geq 0}\) of elements of \( F \) leads to bounds on the number of nonzero entries in each row of the generating matrices. To describe these bounds, we define the length of a row \((c_0, c_1, \ldots) \in \mathbb{F}_q^{N_0}\) with only finitely many nonzero entries by \( \text{max} \{ l \in \mathbb{N} : c_{l-1} \neq 0 \} \), with the proviso that the length is 0 if \( c_r = 0 \) for all \( r \geq 0 \).

**Theorem 2** The generating matrices \( C^{(1)}, \ldots, C^{(s)} \) of the \((g, e, s)\)-sequence in base \( q \) constructed in this section satisfy the property that for all \( 1 \leq i \leq s \)

\[
13
\]
and $d \in \mathbb{N}$, the length of the $d$th row of $C^{(i)}$ is at most
\[ g + sv \left\lfloor \frac{d - 1}{v} \right\rfloor + iv. \]

Here $g$ is the genus of $F$, $e = (e_1, \ldots, e_s)$ with $e_i = \deg(P_i)$ for $1 \leq i \leq s$, and $v = \lcm(e_1, \ldots, e_s)$.

**Proof.** We fix $i \in \{1, \ldots, s\}$ and $d \in \mathbb{N}$ and let $a \in \mathbb{N}_0$ and $w \in \{1, \ldots, v\}$ be such that $d = av + w$. We write $C^{(i)} = \left( c^{(i)}_{j,r} \right)_{j \geq 1, r \geq 0} \in \mathbb{F}_q^{\mathbb{N} \times \mathbb{N}_0}$. In order to ensure that for every $r \geq g + sv \left\lfloor (d - 1)/v \right\rfloor + iv = g + sva + iv$, the entry $c^{(i)}_{d,r}$ in the $d$th row of $C^{(i)}$ is 0, it suffices to show by the construction of $C^{(i)}$ that $\nu_{P_i}(y_r) \geq (a + 1)v/e_i$. (Note that $(a + 1)v \geq d$.) Preliminarily, we consider the case where $r - g \geq sva$ and we see from the definition of $l_s$ that $l_s \geq a$. Now in the case where $r - g \geq sva + iv$, we have either $l_s \geq a + 1$, or otherwise $l_s = a$ and $l_j \geq 1$ for at least one $j \in \{i, i+1, \ldots, s-1\}$. Thus, we always have $l_i + l_{i+1} + \cdots + l_s \geq a + 1$. From $y_r \in \mathcal{L}(D_r)$ we deduce that
\[ \nu_{P_i}(y_r) \geq (l_i + l_{i+1} + \cdots + l_s) \frac{v}{e_i} \geq \frac{(a + 1)v}{e_i}, \]
and this proves our claim. \qed

**Remark 7** In the case where the genus $g$ is 0 and $v = 1$, the matrices $C^{(1)}, \ldots, C^{(s)}$ constructed in this section have asymptotically shortest possible row lengths in the sense of Hofer and Larcher [9, Section 4] (compare also with [7, p. 590], [8, Remark 3], and [17]).

**Remark 8** Given a prime power $q$ and a dimension $s \in \mathbb{N}$, let $F$ be a global function field with full constant field $\mathbb{F}_q$ such that $F$ contains at least $s + 1$ rational places. Then in the construction in this section we can, besides $P_\infty$, also take $P_1, \ldots, P_s$ to be rational places of $F$, that is, $e_i = \deg(P_i) = 1$ for $1 \leq i \leq s$. In this way we obtain a $(t, s)$-sequence in base $q$ with finite-row generating matrices and with $t = g$, the genus of $F$. Now we optimize the construction in the following sense. As in [18, Eq. (10)], we define $V_q(s)$ to be the least $g \in \mathbb{N}_0$ such that there exists a global function field with full constant field $\mathbb{F}_q$, genus $g$, and at least $s + 1$ rational places. Then there exists a $(V_q(s), s)$-sequence in base $q$ with finite-row generating matrices. It was shown in [18, Theorem 4] that $V_q(s) = O(s)$ as $s \to \infty$ with an absolute implied constant. Hence for fixed $q$, we obtain for any dimension $s$ a $(t, s)$-sequence in base $q$ with finite-row generating matrices such that the value of the quality parameter $t$ grows linearly in $s$ as $s \to \infty$. This growth rate
of $t$ is best possible since it is well known that for any fixed base $b$, the least $t$-value $t_b(s)$ of any $(t,s)$-sequence in base $b$ grows at least linearly as a function of $s$ as $s \to \infty$ (see [19, Theorem 8] and [21, Theorem 1]). For the only construction of $(t,s)$-sequences in base $q$ with finite-row generating matrices available for any $q$ and $s$ that was known previously, namely the construction in [8], the least possible value of $t$ grows at the rate $s \log s$ as $s \to \infty$ for fixed $q$.

5 Discrepancy bounds

All known upper bounds on the star discrepancy $D_N^*(S)$ of a $(t,s)$-sequence $S$ in base $b$ are of the form

$$D_N^*(S) \leq c N^{-(\log N)^s} + O(N^{-(\log N)^{s-1}}) \quad \text{for all } N \geq 2,$$

(3)

where the constant $c > 0$ and the implied constant in the Landau symbol depend only on $b$, $s$, and $t$. The classical formulas for $c$ were established by Niederreiter [13, Section 4] and they are summarized in [16, Theorem 4.17]. Later, ameliorated values of $c$ were obtained by Kritzer [10] and Faure and Lemieux [6]. The currently best values of $c$ are those of Faure and Kritzer [5], namely $c = c_{FK}$ given by

$$c_{FK} = \begin{cases} \frac{b^t}{s!} \cdot \frac{b^2}{2(b^2-1)} \left( \frac{b-1}{2 \log b} \right)^s & \text{if } b \text{ is even}, \\ \frac{b^t}{s!} \cdot \frac{1}{2} \left( \frac{b-1}{2 \log b} \right)^s & \text{if } b \text{ is odd}. \end{cases}$$

It follows that for every base $b \geq 2$ we have

$$c_{FK} \geq \frac{b^t}{s!} \cdot \frac{1}{2} \left( \frac{b-1}{2 \log b} \right)^s.$$  

(4)

By applying the signed-splitting technique of Atanassov [1], Tezuka [26] established an upper bound on the star discrepancy $D_N^*(S)$ of a $(u,e,s)$-sequence $S$ in base $b$ which is of the form (3) with the constant $c = c_{Tez}$ given by

$$c_{Tez} = \frac{b^u}{s!} \prod_{i=1}^{s} \frac{b^{e_i}/2}{e_i \log b} \leq \frac{b^u}{s!} \cdot \frac{b^{e_1+\ldots+e_s}}{(2 \log b)^{e_1} \cdot \ldots \cdot e_s}.$$  

(5)

Note that our Definition 2 of a $(u,e,s)$-sequence in base $b$ is slightly stronger than Tezuka’s original definition in [26], and so Tezuka’s discrepancy bound is obviously valid for our concept of a $(u,e,s)$-sequence in base $b$ as well.

The new sequences constructed in Sections 3 and 4 are $(t,s)$-sequences in base $q$ as well as $(u,e,s)$-sequences in base $q$ with suitable $t$, $u$, and $e$. 

15
Therefore we can apply two versions of the discrepancy bound (3), namely the one with $c = c_{FK}$ and the one with $c = c_{Tez}$. It is of interest to compare these two bounds. Recall that for these sequences we have $u = g$, the genus of the global function field $F$, as well as $e = (e_1, \ldots, e_s)$ and $t = g + \sum_{i=1}^{s}(e_i - 1)$, where $e_i = \deg(P_i)$ for $1 \leq i \leq s$. Then from (4) and (5) we obtain

$$\frac{c_{FK}}{c_{Tez}} \geq 1 + \frac{1}{2} \left( \frac{q - 1}{q} \right)^s \prod_{i=1}^{s} e_i.$$  

Thus, if

$$\prod_{i=1}^{s} e_i > 2 \left( \frac{q}{q - 1} \right)^s,$$

then the discrepancy bound with the constant $c_{Tez}$ is better than the one with the constant $c_{FK}$. The condition (6) will be satisfied in many cases.

Consider a typical situation where we fix a global function field $F$ with full constant field $\mathbb{F}_q$ such that $F$ has at least one rational place $P_\infty$. We arrange all distinct places in $\mathbb{F}_F \setminus \{P_\infty\}$ into a list $P_1, P_2, \ldots$ in an arbitrary manner. Then we have the following result.

**Proposition 4** Let $P_1, P_2, \ldots$ be a list of all distinct places in $\mathbb{F}_F \setminus \{P_\infty\}$ as above, where $F$ is a given global function field with full constant field $\mathbb{F}_q$. Then for any $0 < \varepsilon < 1/q$ we have

$$\prod_{i=1}^{s} \deg(P_i) > (\log_q s)^{((1/q) - \varepsilon)s}$$

for all sufficiently large $s$, where $\log_q$ denotes the logarithm to the base $q$.

**Proof.** For any $k \in \mathbb{N}$, let $B_k$ be the number of places of $F$ of degree $k$ and let $T_k = \sum_{h=1}^{k} B_h$ be the number of places of $F$ of degree $\leq k$. Let $f_0 = \deg(P_\infty) = 1, f_1, f_2, \ldots$ be the nondecreasing sequence of positive integers that is obtained by listing each $k \in \mathbb{N}$ with multiplicity $B_k$. Note that $f_0, f_1, f_2, \ldots$ is also the list of the degrees of all places of $F$ in nondecreasing order.

Throughout the proof we assume that $s$ is sufficiently large. Let $j = j(s)$ be the largest $h \in \mathbb{N}$ with $T_h \leq s + 1$. Then

$$\sum_{i=1}^{s} \log \deg(P_i) \geq \sum_{i=1}^{s} \log f_i = \sum_{i=0}^{s} \log f_i \geq \sum_{i=0}^{T_j - 1} \log f_i = \sum_{k=1}^{j} B_k \log k.$$  

(7)
For any $0 < \delta < 1$ we have
\[ \sum_{k=1}^{j} B_k \log k \geq \sum_{k=\lceil j^\delta \rceil}^{j} B_k \log k \geq \delta (T_j - T_{\lceil j^\delta \rceil} - 1) \log j. \] (8)

The Prime Number Theorem for global function fields [11] yields
\[ T_j = \frac{q^j}{q - 1} \cdot \frac{q^j}{j} + o\left(\frac{q^j}{j}\right) \quad \text{as} \; j \to \infty. \] (9)

Noting that with $s$ also $j = j(s)$ is sufficiently large, we deduce from (7), (8), and (9) that for any $0 < \varepsilon_1 < q/(q - 1)$ we have
\[ \sum_{i=1}^{s} \log \deg(P_i) \geq \sum_{k=1}^{j} B_k \log k \geq \left(\frac{q}{q - 1} - \varepsilon_1\right) \frac{q^j}{j} \log j. \]

The definition of $j$ implies that $T_j > s + 1$. Using again (9), we obtain for any $\varepsilon_2 > 0$ that
\[ s < T_{j+1} \leq \left(\frac{q}{q - 1} + \varepsilon_2\right) \frac{q^{j+1}}{j+1} < \left(\frac{q^2}{q - 1} + \varepsilon_2 q\right) \frac{q^j}{j}, \]
and so for any $0 < \varepsilon_3 < (q - 1)/q^2$ we have
\[ \frac{q^j}{j} > \left(\frac{q - 1}{q^2} - \varepsilon_3\right) s. \]

Similarly,
\[ s < T_{j+1} \leq \frac{3q^{j+1}}{j+1} < q^j, \]
and so $j > \log_q s$. By combining these inequalities, we get
\[ \sum_{i=1}^{s} \log \deg(P_i) > \left(\frac{q}{q - 1} - \varepsilon_1\right) \left(\frac{q - 1}{q^2} - \varepsilon_3\right) s \log \log_q s. \]

Now for a given $0 < \varepsilon < 1/q$ we can choose $\varepsilon_1$ and $\varepsilon_3$ suitably small such that
\[ \left(\frac{q}{q - 1} - \varepsilon_1\right) \left(\frac{q - 1}{q^2} - \varepsilon_3\right) \geq \frac{1}{q} - \varepsilon. \]
Consequently,
\[ \sum_{i=1}^{s} \log \deg(P_i) > \left(\frac{1}{q} - \varepsilon\right) s \log \log_q s \]
for all sufficiently large $s$, and this implies the desired result. □
If we now take for the given global function field \( F \) and a given \( s \in \mathbb{N} \) the first \( s \) places \( P_1, \ldots, P_s \) from the list \( P_1, P_2, \ldots \) in Proposition 4, then it follows from this result that the condition (6) is satisfied for all sufficiently large \( s \).

Remark 9 In view of Remark [6], the discussion in this section applies in exactly the same way to upper bounds on the star discrepancy of the Niederreiter-Xing sequences constructed in [27].

References

[1] E.I. Atanassov, On the discrepancy of the Halton sequences, Math. Balkanica New Series 18 (2004) 15–32.

[2] J. Dick, H. Niederreiter, On the exact \( t \)-value of Niederreiter and Sobol’ sequences, J. Complexity 24 (2008) 572–581.

[3] J. Dick, F. Pillichshammer, Digital Nets and Sequences: Discrepancy Theory and Quasi-Monte Carlo Integration, Cambridge University Press, Cambridge, 2010.

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

[5] H. Faure, P. Kritzer, New star discrepancy bounds for \((t, m, s)\)-nets and \((t, s)\)-sequences, preprint, 2012.

[6] H. Faure, C. Lemieux, Improvements on the star discrepancy of \((t, s)\)-sequences, Acta Arith. 154 (2012) 61–78.

[7] R. Hofer, A construction of digital \((0, s)\)-sequences involving finite-row generator matrices, Finite Fields Appl. 18 (2012) 587–596.

[8] R. Hofer, A construction of low-discrepancy sequences involving finite-row digital \((t, s)\)-sequences, Monatsh. Math., to appear; DOI 10.1007/s00605-012-0439-0.

[9] R. Hofer, G. Larcher, On existence and discrepancy of certain digital Niederreiter-Halton sequences, Acta Arith. 141 (2010) 369–394.

[10] P. Kritzer, Improved upper bounds on the star discrepancy of \((t, m, s)\)-nets and \((t, s)\)-sequences, J. Complexity 22 (2006) 336–347.
[11] M. Kruse, H. Stichtenoth, Ein Analogon zum Primzahlsatz für algebraische Funktionenkörper, Manuscripta Math. 69 (1990) 219–221.

[12] D.J.S. Mayor, H. Niederreiter, A new construction of \((t, s)\)-sequences and some improved bounds on their quality parameter, Acta Arith. 128 (2007) 177–191.

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

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

[15] H. Niederreiter, Quasi-Monte Carlo methods for multidimensional numerical integration, in: H. Braß, G. Hämmerlin (Eds.), Numerical Integration III, International Series of Numerical Mathematics, vol. 85, Birkhäuser, Basel, 1988, pp. 157–171.

[16] H. Niederreiter, Random Number Generation and Quasi-Monte Carlo Methods, CBMS-NSF Regional Conference Series in Applied Mathematics, vol. 63, SIAM, Philadelphia, 1992.

[17] H. Niederreiter, Finite fields and quasirandom points, in: P. Charpin, A. Pott, A. Winterhof (Eds.), Finite Fields and Applications: Character Sums and Polynomials, Radon Series on Computational and Applied Mathematics, W. de Gruyter, Berlin, to appear.

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

[19] H. Niederreiter, C.P. Xing, Quasirandom points and global function fields, in: S. Cohen, H. Niederreiter (Eds.), Finite Fields and Applications, Cambridge University Press, Cambridge, 1996, pp. 269–296.

[20] H. Niederreiter, C.P. Xing, Rational Points on Curves over Finite Fields: Theory and Applications, Cambridge University Press, Cambridge, 2001.

[21] R. Schürer, A new lower bound on the \(t\)-parameter of \((t, s)\)-sequences, in: A. Keller, S. Heinrich, H. Niederreiter (Eds.), Monte Carlo and Quasi-Monte Carlo Methods 2006, Springer, Berlin, 2008, pp. 623–632.

[22] I.M. Sobol’, Distribution of points in a cube and approximate evaluation of integrals (Russian), Ž. Vyčisl. Mat. i Mat. Fiz. 7 (1967) 784–802.
[23] H. Stichtenoth, Algebraic Function Fields and Codes, 2nd ed., Springer, Berlin, 2009.

[24] S. Tezuka, Polynomial arithmetic analogue of Halton sequences, ACM Trans. Modeling Computer Simulation 3 (1993) 99–107.

[25] S. Tezuka, Uniform Random Numbers: Theory and Practice, Kluwer Academic Publishers, Boston, 1995.

[26] S. Tezuka, On the discrepancy of generalized Niederreiter sequences, preprint, 2012.

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

Roswitha Hofer, Institute of Financial Mathematics, University of Linz, Altenbergerstr. 69, A-4040 Linz, Austria; email: roswitha.hofer@jku.at

Harald Niederreiter, Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstr. 69, A-4040 Linz, Austria, and Department of Mathematics, University of Salzburg, Hellbrunnerstr. 34, A-5020 Salzburg, Austria; email: ghnied@gmail.com