Explicit constructions of Vandermonde sequences using global function fields

Roswitha Hofer and Harald Niederreiter

Abstract

The authors recently introduced so-called Vandermonde nets. These digital nets share properties with the well-known polynomial lattices. For example, both can be constructed via component-by-component search algorithms. A striking characteristic of the Vandermonde nets is that for fixed \( m \) an explicit construction of \( m \times m \) generating matrices over the finite field \( \mathbb{F}_q \) is known for dimensions \( s \leq q + 1 \). This paper extends this explicit construction in two directions. We give a maximal extension in terms of \( m \) by introducing a construction algorithm for \( \infty \times \infty \) generating matrices for digital sequences over \( \mathbb{F}_q \), which works in the rational function field over \( \mathbb{F}_q \). Furthermore, we generalize this method to global function fields of positive genus, which leads to extensions in the dimension \( s \).

Keywords: Low-Discrepancy Sequences, Digital Sequences, Generating Matrices, Global Function Field.

MSC2010: 11K31, 11K38, 14G15.

1 Introduction

The authors \cite{Hofer96} recently introduced a new family of digital \((t, m, s)\)-nets called Vandermonde nets. In the present paper, we expand on this work. We consider chains of embedded Vandermonde nets or, equivalently, digital \((T, s)\)-sequences with generating matrices possessing a Vandermonde-type structure. This leads to new constructions of digital \((T, s)\)-sequences. We refer to the monograph \cite{Niederreiter92} and the recent handbook article \cite{Hofer08} for the necessary background on digital \((t, m, s)\)-nets and digital \((T, s)\)-sequences.

We start out by giving an explicit construction, using the rational function field \( \mathbb{F}_q(x) \) over the finite field \( \mathbb{F}_q \), of chains of embedded Vandermonde nets (we may equivalently speak of Vandermonde sequences) which is based on methods and tools available in global function fields. Here the exponents appearing in the Vandermonde-type matrices are translated to multiples of selected divisors in Section\cite{Hofer96}. This relation to the Vandermonde structure is pointed out in Remark\cite{Niederreiter92}. 

1
Section 3 gives a generalized version of the construction in global function fields with positive genus $g$. Finally, Section 4 shows how, in the specific case where the entries of the generating matrices stem from local expansions at a rational place, it is possible to reach the usual best known quality parameter $t = g$, where $g$ is the genus of the underlying global function field. Concerning global function fields, we follow the notation and terminology in the book [5].

Throughout this paper we use the convention that empty sums are considered to be 0. Other statements or conditions depending on an empty index set (e.g. $j$ in the range $1 \leq j \leq 0$) are disregarded.

2 Embedded explicit construction in $\mathbb{F}_q(x)$

Let $s \geq 2$ be an integer and let $P_1, \ldots, P_s, P_\infty$ be distinct places of the rational function field $\mathbb{F}_q(x)$, where $P_1, \ldots, P_s$ are rational and $P_\infty$ has an arbitrary degree $\mu$. Note $s \leq q + 1$. (For example, choose $P_1$ as the infinite place of $\mathbb{F}_q(x)$ and $P_2, \ldots, P_s$ as places corresponding to distinct monic linear polynomials $p_2(x), \ldots, p_s(x)$, say $p_2(x) = x + c_2 = x, p_3(x) = x + c_3, \ldots, p_s(x) = x + c_s$, and let $P_\infty$ correspond to a further monic irreducible polynomial $p_\infty(x)$ of degree $\mu$.) The generating matrices $C^{(1)}, \ldots, C^{(s)} \in \mathbb{F}_q^{N \times N_0}$ are constructed row by row as follows. Choose

$$\beta_j^{(1)} \in \mathcal{L}(j(P_1 - P_2)) \setminus \{0\}$$

and

$$\beta_j^{(i)} \in \mathcal{L}(j(P_i - P_1)) \setminus \{0\}$$

for $j \geq 1$ and $i \in \{2, \ldots, s\}$. (In the example, one possible setting is $\beta_j^{(1)} = x^{j-1}$ and $\beta_j^{(i)} = 1/(x + c_i)^j$ for $j \geq 1, 2 \leq i \leq s$.)

**Lemma 1** Such $\beta_j^{(i)}$ exist for every $j \geq 1$ and $1 \leq i \leq s$. We have

1. $\nu_{P_1}(\beta_j^{(1)}) = -j + 1$,
2. $\nu_{P_2}(\beta_j^{(1)}) = j - 1$,
3. $\nu_{P_1}(\beta_j^{(i)}) = -j$, and
4. $\nu_{P_1}(\beta_j^{(i)}) = j$

for $j \geq 1$ and $2 \leq i \leq s$. Furthermore, the system $\{\beta_j^{(i)}\}_{1 \leq i \leq s, j \geq 1}$ is linearly independent over $\mathbb{F}_q$. 

2
Proof. Existence follows from the Riemann-Roch theorem \[5\] Theorem 1.5.17] since \(\deg(P_i - P_h) = 0\) for every choice of \(1 \leq i, h \leq s\), and therefore the dimension of \(\mathcal{L}(P_i - P_h)\) is 1. The values of the valuations follow directly from the construction of \(\beta^{(i)}_j\) together with the fact that the degree of a principal divisor is 0. The linear independence is now easily seen using the known values of the valuations at the places. \(\square\)

Remark 1 An alternative version would be to choose \(\alpha_1 \in \mathcal{L}(P_1 - P_2) \setminus \{0\}\) and \(\alpha_i \in \mathcal{L}(P_i - P_1) \setminus \{0\}\) for \(2 \leq i \leq s\) and set \(\beta^{(1)}_j = \alpha^{-1}_1\) and \(\beta^{(i)}_j = \alpha^i_j\) for \(j \geq 1\) and \(2 \leq i \leq s\), in order to obtain a Vandermonde structure of the matrix \(C\) that determines the rows, i.e.,

\[
C = \begin{pmatrix}
1 & \alpha_1 & \alpha_1^2 & \cdots \\
\alpha_2 & \alpha_2^2 & \alpha_2^3 & \cdots \\
\vdots & \vdots & \vdots & \ddots \\
\alpha_s & \alpha_s^2 & \alpha_s^3 & \cdots \\
\end{pmatrix} \in \mathbb{F}_q^s \times \mathbb{N}.
\]

This conforms with the theory of Vandermonde nets developed in \[2\]. This choice is covered by the example at the beginning of this section, but is not adaptable to global function fields with positive genus. Note that the pole divisor of \(\beta^{(2)}_1\) would be \(P_2\), but this is impossible by the Weierstrass gap theorem \[5\] Theorem 1.6.8] which states that in the case of a positive genus, the integer 1 has to be a gap number of the rational place \(P_2\).

The \(j\)th row of \(C^{(i)}\) is determined by the coefficients of the local expansion of \(\beta^{(i)}_j\) at the place \(P_\infty\), which is of the form

\[
\beta^{(i)}_j = \sum_{k=0}^{\infty} a^{(i)}_{j,k} z^k,
\]

where \(z = p_\infty(x)\) is a local parameter at \(P_\infty\) and \(a^{(i)}_{j,k} \in \{f(x) \in \mathbb{F}_q[x] : \deg(f(x)) < \mu\}\) for \(k \geq 0\). Note that the construction ensures \(\nu_{P_\infty}(\beta^{(i)}_j) \geq 0\) for all \(j \geq 1\) and \(1 \leq i \leq s\) and the set \(\{f(x) \in \mathbb{F}_q[x] : \deg(f(x)) < \mu\}\) forms a vector space over \(\mathbb{F}_q\) with basis \(1, x, \ldots, x^{\mu-1}\). (Note the linearity of the local expansion over \(\mathbb{F}_q\).) Now identify \(a^{(i)}_{j,k}\) with a vector in \(\mathbb{F}_q^\mu\) with respect to the basis \(1, x, \ldots, x^{\mu-1}\) and build the row \(c^{(i)}_j\) by concatenating these vectors.

Before describing the quality of this construction in Theorem [II] below, we note the following general fact about digital \((T, s)\)-sequences.

**Lemma 2** Let \(\mu, s \in \mathbb{N}\) and let \(C^{(1)}, \ldots, C^{(s)}\) be generating matrices of a digital \((T, s)\)-sequence over \(\mathbb{F}_q\). If \(T(\ell, \mu) \leq t\) for some \(t \in \mathbb{N}_0\) and every \(\ell \in \mathbb{N}\), then \(T : \mathbb{N} \to \mathbb{N}_0\) is given by \(T(m) = \min(m, t + r(m))\), where \(r(m)\) is the least residue of \(m\) mod \(\mu\).
Proof. This easily follows from the definition of $T : \mathbb{N} \to \mathbb{N}_0$ depending on the rank structure of $C^{(1)}, \ldots, C^{(s)}$. \hfill \Box

Theorem 1 The matrices $C^{(1)}, \ldots, C^{(s)}$ constructed in this section generate a digital $(T, s)$-sequence over $\mathbb{F}_q$ with $T(m) = r(m)$, where $r(m)$ is the least residue of $m \mod \mu$.

Proof. Because of Lemma 2 it suffices to prove $T(\ell \mu) = 0$ for every $\ell \in \mathbb{N}$, i.e., to ensure for every choice of $\ell \in \mathbb{N}$ and $d_1, \ldots, d_s \in \mathbb{N}_0$ satisfying $1 \leq d_1 + \cdots + d_s \leq \ell \mu$ that the matrix formed by the row vectors

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

with $1 \leq j \leq d_i$, $1 \leq i \leq s$, and $m = \ell \mu$ has full row rank $d_1 + \cdots + d_s$. Suppose that

$$\sum_{i=1}^s \sum_{j=1}^{d_i} b_j^{(i)} c_j^{(i, m)} = 0 \in \mathbb{F}_q^m$$

for some $b_j^{(i)} \in \mathbb{F}_q$. The linearity of the local expansion yields

$$\beta := \sum_{i=1}^s \sum_{j=1}^{d_i} b_j^{(i)} \beta_j^{(i)} = \sum_{k=0}^\infty \left( \sum_{i=1}^s \sum_{j=1}^{d_i} b_j^{(i)} a_{j,k}^{(i)} \right) z^k.$$

Using (1) together with the construction principle, we obtain

$$\beta = \sum_{k=\ell}^{\infty} \left( \sum_{i=1}^s \sum_{j=1}^{d_i} b_j^{(i)} a_{j,k}^{(i)} \right) z^k.$$

Thus $\nu_{\mathbb{F}_q}(\beta) \geq \ell$.

We observe that

$$\beta_j^{(1)} \in \mathcal{L}((j - 1)(P_1 - P_2)) \subseteq \mathcal{L}((d_1 - 1)P_1 + d_2 P_2 + \cdots + d_s P_s)$$

for every $1 \leq j \leq d_1$ and that

$$\beta_j^{(i)} \in \mathcal{L}(jP_i - jP_1) \subseteq \mathcal{L}(d_i P_i - P_1) \subseteq \mathcal{L}((d_1 - 1)P_1 + d_2 P_2 + \cdots + d_s P_s)$$

for $1 \leq j \leq d_i$, $2 \leq i \leq s$. This together with $\nu_{\mathbb{F}_q}(\beta) \geq \ell$ implies that

$$\beta \in \mathcal{L}((d_1 - 1)P_1 + d_2 P_2 + \cdots + d_s P_s - \ell P_\infty) =: \mathcal{L}(D_{m,d_1,\ldots,d_s}).$$

Finally, we compute the degree of $D_{m,d_1,\ldots,d_s}$ and obtain

$$\deg(D_{m,d_1,\ldots,d_s}) = \left( \sum_{i=1}^s d_s \right) - 1 - \ell \mu \leq \ell \mu - 1 - \ell \mu = -1.$$ 

Thus $\beta = 0$. Finally, the linear independence of the system $\{\beta_j^{(i)}\}_{1 \leq i \leq s, j \geq 1}$, ensured by Lemma 1, implies that $b_j^{(i)} = 0$ for $1 \leq j \leq d_i$, $1 \leq i \leq s$. \hfill \Box
Remark 2 In the case where \( \mu = 2 \), the construction in this section provides a digital \((T, q + 1)\)-sequence over \( \mathbb{F}_q \) with \( T(m) = 0 \) for even \( m \) and \( T(m) = 1 \) for odd \( m \). This construction is substantially simpler than the one introduced by Niederreiter and Özbudak in [4] with the same function \( T \).

3 Generalization to \( g > 0 \)

Let \( F \) be a global function field with full constant field \( \mathbb{F}_q \) and genus \( g > 0 \). Let \( s \geq 2 \) be an integer and let \( P_1, \ldots, P_s, P_\infty \) be distinct places of \( F \), where \( P_1, \ldots, P_s \) are rational and \( P_\infty \) has an arbitrary degree \( \mu \). We additionally use a positive auxiliary divisor \( D \) of \( F \) with \( \deg(D) = 2g \) and \( \text{supp}(D) \cap \{P_\infty, P_2, \ldots, P_s\} = \emptyset \) (e.g. \( D = 2gP_1 \)). We choose

\[
\beta^{(1)}_j \in \mathcal{L}(D + (j - 1)P_1 - (j - 1)P_2) \setminus \mathcal{L}(D + (j - 2)P_1 - (j - 1)P_2)
\]

and

\[
\beta^{(i)}_j \in \mathcal{L}(D + jP_i - jP_1) \setminus (\mathcal{L}(D + jP_i - (j + 1)P_1) \cup \mathcal{L}(D + (j - 1)P_i - jP_1))
\]

for \( j \geq 1 \) and \( 2 \leq i \leq s \).

Lemma 3 Such \( \beta^{(i)}_j \) exist for every \( j \geq 1 \) and \( 1 \leq i \leq s \). We have

1. \( \nu_{P_i}(\beta^{(1)}_j) = -(j - 1) - \nu_{P_i}(D) \),
2. \( \nu_{P_i}(\beta^{(i)}_j) \geq 0 \),
3. \( \nu_{P_i}(\beta^{(i)}_j) = -j \), and
4. \( \nu_{P_i}(\beta^{(i)}_j) = j - \nu_{P_i}(D) \)

for \( j \geq 1 \), for \( 2 \leq i \leq s \), and for \( 2 \leq h \leq s \), \( 1 \leq l \leq s \) satisfying \( h \neq l \). Furthermore, the system \( \{\beta^{(i)}_j\}_{1 \leq i \leq s, j \geq 1} \) is linearly independent over \( \mathbb{F}_q \).

Proof. The values of the valuations follow directly from the construction of \( \beta^{(i)}_j \) and from the special choice of \( D \). We observe that

\[
\deg(\mathcal{L}(D + (j - 1)P_1 - (j - 1)P_2)) = 2g,
\]

\[
\deg(\mathcal{L}(D + (j - 2)P_1 - (j - 1)P_2)) = 2g - 1,
\]

\[
\deg(\mathcal{L}(D + jP_i - jP_1)) = 2g,
\]

\[
\deg(\mathcal{L}(D + (j - 1)P_i - jP_1)) = 2g - 1,
\]

\[
\deg(\mathcal{L}(D + jP_i - (j + 1)P_1)) = 2g - 1,
\]

\[
(\mathcal{L}(D + jP_i - (j + 1)P_1) \cap \mathcal{L}(D + (j - 1)P_i - jP_1)) \supseteq \{0\}.
\]
Existence of $\beta_j^{(i)}$ for $j \geq 1$ follows directly from the Riemann-Roch theorem together with (2) and (3). Existence of $\beta_j^{(i)}$ for $j \geq 1, 2 \leq i \leq s$ follows from

$$|L(D + jP_1 - jP_1)| - |L(D + (j - 1)P_1 - jP_1)| - |L(D + jP_1 - (j + 1)P_1)| + |L(D + jP_1 - (j + 1)P_1) \cap L(D + (j - 1)P_1 - jP_1)| \geq q^{g+1} - q^g - q^g + 1 \geq 1,$$

where we used the Riemann-Roch theorem together with (4), (5), (6), and (7).

The values of the valuations can be used to see the linear independence of the $\beta_j^{(i)}$. $\square$

The $j$th row of $C(i)$ is determined by the coefficients of the local expansion of $\beta_j^{(i)}$ at the place $P_\infty$, which is of the form

$$\beta_j^{(i)} = \sum_{k=0}^{\infty} a_{j,k}^{(i)} z^k,$$

where $z$ is a local parameter at $P_\infty$ and the coefficients $a_{j,k}^{(i)}$ are chosen in a set of representatives, which ensures linearity of the local expansion and that each representative can be uniquely identified with a vector in $\mathbb{F}_q^\mu$. Now build the $j$th row $c_j^{(i)}$ of $C(i)$ by concatenating these vectors. Note that the construction guarantees $\nu_{P_\infty}(\beta_j^{(i)}) \geq 0$ for all $j \geq 1$ and $1 \leq i \leq s$.

**Theorem 2** The matrices $C^{(1)}, \ldots, C^{(s)}$ constructed in this section generate a digital $(T, s)$-sequence over $\mathbb{F}_q$ with $T(m) = \min(m, 2g + r(m))$, where $r(m)$ is the least residue of $m$ mod $\mu$.

**Proof.** Because of Lemma [2] it suffices to prove $T(\ell \mu) \leq 2g$ for every $\ell \in \mathbb{N}$, i.e., to ensure for every choice of $\ell \in \mathbb{N}$ satisfying $\ell \mu > 2g$ and of $d_1, \ldots, d_s \in \mathbb{N}_0$ satisfying $1 \leq d_1 + \cdots + d_s \leq \ell \mu - 2g$ that the matrix formed by the row vectors

$$c_j^{(i,m)} := (c_j^{(i,0)}, \ldots, c_j^{(i,m-1)}) \in \mathbb{F}_q^m$$

with $1 \leq j \leq d_i, 1 \leq i \leq s$, and $m = \ell \mu$ has full row rank $d_1 + \cdots + d_s$.

Suppose that

$$\sum_{i=1}^s \sum_{j=1}^{d_i} b_j^{(i)} c_j^{(i,m)} = 0 \in \mathbb{F}_q^m$$

for some $b_j^{(i)} \in \mathbb{F}_q$. The linearity of the local expansion yields

$$\beta := \sum_{i=1}^s \sum_{j=1}^{d_i} b_j^{(i)} \beta_j^{(i)} = \sum_{k=0}^{\infty} \left( \sum_{i=1}^s \sum_{j=1}^{d_i} b_j^{(i)} a_{j,k}^{(i)} \right) z^k.$$
Using (8) together with the construction principle, we obtain

\[ \beta = \sum_{k=\ell}^{\infty} \left( \sum_{i=1}^{s} \sum_{j=1}^{d_i} b_j^{(i)} a_{j,k}^{(i)} \right) z^k. \]

Therefore \( \nu_{P_\infty}(\beta) \geq \ell. \)

Note that

\[ \beta_j^{(1)} \in \mathcal{L}(D+(j-1)P_1-(j-1)P_2) \subseteq \mathcal{L}(D+(j-1)P_1) \subseteq \mathcal{L}(D+(d_1-1)P_1+d_2P_2+\cdots+d_sP_s) \]

for \( 1 \leq j \leq d_1 \) and

\[ \beta_j^{(i)} \in \mathcal{L}(D+jP_i-jP_1) \subseteq \mathcal{L}(D+d_iP_i-P_1) \subseteq \mathcal{L}(D+(d_1-1)P_1+d_2P_2+\cdots+d_sP_s) \]

for \( 1 \leq j \leq d_i, \ 2 \leq i \leq s. \) This together with \( \nu_{P_\infty}(\beta) \geq \ell \) implies that

\[ \beta \in \mathcal{L}(D+(d_1-1)P_1+d_2P_2+\cdots+d_sP_s-\ell P_\infty) =: \mathcal{L}(D_{m,d_1,\ldots,d_s}). \]

We observe that

\[ \deg(D_{m,d_1,\ldots,d_s}) \leq 2g+m-2g-1-m = -1 \]

which implies that \( \beta = 0. \) Finally, the linear independence of the system \( \{\beta_j^{(i)}\}_{1 \leq i \leq s, j \geq 1}, \)

ensured by Lemma 3 yields \( b_j^{(i)} = 0 \) for \( 1 \leq j \leq d_i, \ 1 \leq i \leq s. \)

\[ \square \]

4 The case where \( g > 0 \) and \( P_\infty \) is rational

Here a similar trick as used in the Xing-Niederreiter construction \( [6] \) is available to save an additive term \( g \) in the quality-parameter function \( T. \) Let \( F \) be a global function field with full constant field \( \mathbb{F}_q \) and genus \( g > 0. \) Let \( s \geq 2 \) be an integer and let \( P_1, \ldots, P_s, P_\infty \) be distinct rational places of \( F. \)

Analogously to the last section, we use a positive auxiliary divisor \( D \) of \( F \) with \( \deg(D) = 2g \) and \( \text{supp}(D) \cap \{P_\infty, P_2, \ldots, P_s\} = \emptyset \) (e.g. \( D = 2gP_1 \)) and choose

\[ \beta_j^{(1)} \in \mathcal{L}(D+(j-1)P_1-(j-1)P_2) \setminus \mathcal{L}(D+(j-2)P_1-(j-1)P_2) \]

and

\[ \beta_j^{(i)} \in \mathcal{L}(D+jP_i-jP_1) \setminus (\mathcal{L}(D+jP_i-(j+1)P_1) \cup \mathcal{L}(D+(j-1)P_i-jP_1)), \]

for \( j \geq 1 \) and \( 2 \leq i \leq s. \) Note that the construction and the restriction on \( D \)

ensure \( \nu_{P_\infty}(\beta_j^{(i)}) \geq 0. \) Note that Lemma 3 is valid.

Similarly to the Xing-Niederreiter construction, we construct a basis \( \{w_1, \ldots, w_g\} \)

of the vector space \( \mathcal{L}(D-P_1) \) with dimension \( l(D-P_1) = g \) as follows.
By the Riemann-Roch theorem, we know the dimensions
\[ l(D - P_1) = g \]
and
\[ l(D - P_1 - 2gP_\infty) = 0, \]
therefore there exist integers \(0 \leq n_1 < \cdots < n_g < 2g\) such that
\[ l(D - P_1 - n_fP_\infty) = l(D - P_1 - (n_f + 1)P_\infty) + 1 \] for \(1 \leq f \leq g\).

Now choose \(w_f \in L(D - P_1 - n_fP_\infty) \setminus L(D - P_1 - (n_f + 1)P_\infty)\) to obtain the basis
\[ \{w_1, \ldots, w_g\} \] of \(L(D - P_1)\).

Note that \(\nu_{P_\infty}(w_f) = n_f, \nu_{P_1}(w_f) \geq 1 - \nu_{P_1}(D),\) and \(\nu_{P_i}(w_f) \geq 0\) for every \(2 \leq i \leq s, 1 \leq f \leq g\).

**Lemma 4** The system \(\{w_1, \ldots, w_g\} \cup \{\beta_j^{(i)}\}_{1 \leq i \leq s, j \geq 1}\) is linearly independent over \(\mathbb{F}_q\).

**Proof.** The linear independence of \(\{w_1, \ldots, w_g\}\) and of \(\{\beta_j^{(i)}\}_{j \geq 1}\) for every fixed \(i = 1, \ldots, s\) is obvious. Suppose that
\[ \sum_{f=1}^{g} a_f w_f + \sum_{i=1}^{s} \sum_{j=1}^{v} b_j^{(i)} \beta_j^{(i)} = 0 \]
for some \(v \geq 1\) and \(a_f, b_j^{(i)} \in \mathbb{F}_q\). For a fixed \(h = 2, \ldots, s\), we consider
\[ \sum_{j=1}^{v} b_j^{(h)} \beta_j^{(h)} = - \sum_{f=1}^{g} a_f w_f - \sum_{i \neq h}^{s} \sum_{j=1}^{v} b_j^{(i)} \beta_j^{(i)}. \]

We abbreviate the left-hand side by \(\beta\). Now if \(\beta \neq 0\), we know from Lemma 3 that \(\nu_{P_h}(\beta) < 0\). But the right-hand side satisfies \(\nu_{P_h}(\beta) \geq 0\), hence all coefficients on the left-hand side have to be 0. We arrive at
\[ \sum_{j=1}^{v} b_j^{(1)} \beta_j^{(1)} = - \sum_{f=1}^{g} a_f w_f. \]

We abbreviate the left-hand side by \(\gamma\). If there is a \(b_j^{(1)} \neq 0\) for at least one \(j \geq 1\), then the left-hand side yields \(\nu_{P_1}(\gamma) \leq -\nu_{P_1}(D)\), but the right-hand side shows \(\nu_{P_1}(\gamma) \geq -\nu_{P_1}(D) + 1\). Hence all \(a_f\) and all \(b_j^{(1)}\) have to be 0. \(\square\)

The \(j\)th row of \(C^{(i)}\) is determined by the coefficients of the local expansion of \(\beta_j^{(i)}\) at the rational place \(P_\infty\), which is of the form
\[ \beta_j^{(i)} = \sum_{k=0}^{\infty} a_j^{(i,k)} z_k, \]
where the coefficients \( a_{j,k}^{(i)} \in \mathbb{F}_q \) for \( k \geq 0, j \geq 1, 1 \leq i \leq s \). The sequence \((z_k)_{k \geq 0}\) satisfies for \( k \in \mathbb{N}_0 \setminus \{n_1, \ldots, n_g\} \) that \( \nu_{\mathbb{F}_q}(z_k) = k \), and for \( k = n_f \) with \( f \in \{1, \ldots, g\} \) that \( z_k = w_f \). This preliminary construction yields the following sequence in \( \mathbb{F}_q^s \):

\[
(a_{j,0}^{(i)}, \ldots, a_{j,n_1}^{(i)}, a_{j,n_1+1}^{(i)}, \ldots, a_{j,n_g}^{(i)}, a_{j,n_g+1}^{(i)}, \ldots) \in \mathbb{F}_q^{N_0}.
\]

After deleting the terms with the hat, we arrive at a sequence which serves as the \( j \)th row \( c_{j}^{(i)} \) of \( C^{(i)} \), and we write

\[
c_{j}^{(i)} = (c_{j,0}^{(i)}, c_{j,1}^{(i)}, \ldots) \in \mathbb{F}_q^{N_0}.
\]

**Theorem 3** The matrices \( C^{(1)}, \ldots, C^{(s)} \) constructed in this section generate a digital \((t, s)\)-sequence over \( \mathbb{F}_q \) with \( t = g \).

**Proof.** We prove for every integer \( m > g \) and every choice of nonnegative integers \( d_1, \ldots, d_s \) satisfying \( 1 \leq d_1 + \cdots + d_s \leq m - g \) that the matrix formed by the row vectors

\[
c_{j}^{(i,m)} := (c_{j,0}^{(i)}, \ldots, c_{j,m-1}^{(i)}) \in \mathbb{F}_q^m
\]

with \( 1 \leq j \leq d_i, 1 \leq i \leq s \), has full row rank \( d_1 + \cdots + d_s \).

Choose \( b_{j}^{(i)} \in \mathbb{F}_q \) for \( 1 \leq j \leq d_i, 1 \leq i \leq s \), satisfying

\[
\sum_{i=1}^{s} \sum_{j=1}^{d_i} b_{j}^{(i)} c_{j}^{(i,m)} = 0 \in \mathbb{F}_q^m. \tag{9}
\]

The linearity of the local expansion implies that

\[
\beta := \sum_{i=1}^{s} \sum_{j=1}^{d_i} b_{j}^{(i)} \beta_{j}^{(i)} - \sum_{i=1}^{s} \sum_{j=1}^{d_i} b_{j}^{(i)} \sum_{f=1}^{g} a_{j,n_f}^{(i)} w_f = \sum_{k=0}^{\infty} \left( \sum_{i=1}^{s} \sum_{j=1}^{d_i} b_{j}^{(i)} a_{j,k}^{(i)} \right) z_k.
\]

In view of the construction algorithm and (9), we obtain

\[
\beta = \sum_{k=m+g}^{\infty} \left( \sum_{i=1}^{s} \sum_{j=1}^{d_i} b_{j}^{(i)} a_{j,k}^{(i)} \right) z_k.
\]

Therefore \( \nu_{\mathbb{F}_q}(\beta) \geq m + g \).

We observe that

\[
\alpha \in \mathcal{L}(D - P_1) \subseteq \mathcal{L}(D + (d_1 - 1)P_1 + d_2P_2 + \cdots + d_sP_s),
\]

\[
\beta_{j}^{(1)} \in \mathcal{L}(D + (j-1)P_1 - (j-1)P_2) \subseteq \mathcal{L}(D + (d_1 - 1)P_1 + d_2P_2 + \cdots + d_sP_s)
\]
for $1 \leq j \leq d_1$, and
\[ \beta^{(i)}_{j} \in \mathcal{L}(D+jP_i-P_1) \subseteq \mathcal{L}(D+d_iP_i-P_1) \subseteq \mathcal{L}(D+(d_1-1)P_1+d_2P_2+\cdots+d_sP_s) \]
for $1 \leq j \leq d_i$, $2 \leq i \leq s$. This together with $\nu_{P_{\infty}}(\beta) \geq m + g$ implies that
\[ \beta \in \mathcal{L}(D+(d_1-1)P_1+d_2P_2+\cdots+d_sP_s-(m+g)P_{\infty}) =: \mathcal{L}(D_{m,d_1,\ldots,d_s}). \]

We compute the degree of $D_{m,d_1,\ldots,d_s}$ and obtain
\[ \deg(D_{m,d_1,\ldots,d_s}) \leq 2g + m - g - 1 - (m + g) = -1, \]
which entails $\beta = 0$. Finally, the linear independence of the system \( \{w_1, \ldots, w_g\} \cup \{\beta^{(i)}_{j}\}_{1 \leq i \leq s, j \geq 1} \) yields \( b^{(i)}_{j} = 0 \) for $1 \leq j \leq d_i$, $1 \leq i \leq s$. \( \square \)

References

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

[2] R. Hofer, H. Niederreiter. Vandermonde nets. Preprint, 2013; available at [http://arxiv.org/abs/1308.1215](http://arxiv.org/abs/1308.1215).

[3] H. Niederreiter. \((t, m, s)\)-nets and \((t, s)\)-sequences. Handbook of Finite Fields (G.L. Mullen and D. Panario, eds.), pp. 619–630, CRC Press, Boca Raton, FL, 2013.

[4] H. Niederreiter, F. Özbudak. Low-discrepancy sequences using duality and global function fields. *Acta Arith.*, 130 (2007), 79–97.

[5] H. Stichtenoth. Algebraic Function Fields and Codes, 2nd ed. Springer, Berlin, 2009.

[6] 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