Duality Theory and Propagation Rules for Generalized Digital Nets

Josef Dick and Peter Kritzer

August 29, 2008

Abstract

Digital nets are used in quasi-Monte Carlo algorithms for approximating high dimensional integrals over the unit cube. Hence one wants to have explicit constructions of digital nets of high quality. In this paper we consider so-called propagation rules for digital nets, which state how one can obtain a new digital net of different size from existing digital nets. This way one often can generate digital nets of higher quality than were previously known. Here we generalize existing propagation rules for classical digital nets to generalized digital nets as introduced by Dick.

Keywords: Quasi-Monte Carlo, Numerical Integration, Digital nets, Duality Theory, Propagation Rules

MSC 2000: 11K38, 11K45, 65C05, 94B05

1 Introduction

Often it is necessary to approximate a high dimensional integral \( \int_{[0,1]^s} f(x) \, dx \) by some numerical algorithm. One way of doing so is by using a quasi-Monte Carlo (qMC) algorithm, where one simply approximates the integral by \( \frac{1}{N} \sum_{h=0}^{N-1} f(x_h) \). As quadrature points one can use a so-called digital \((t, m, s)\)-net. Classical digital \((t, m, s)\)-nets were introduced by Niederreiter [6] (see also [7]). The aim of these constructions is to obtain point sets which are uniformly distributed in \([0,1]^s\). By a point set we mean a multiset, i.e., points may occur repeatedly. One obtains the optimal order of convergence (up to powers of the logarithm of the total number of points) in this case for functions which have finite variation in the sense of Hardy and Krause, see [7].

In [4] digital nets were generalized to construct point sets for which the corresponding qMC algorithm achieves higher order convergence of the integration error for smoother functions. The construction principle of a digital net in the sense of [6] and [4] is based on linear algebra over finite fields and works as follows. Here and in the following, vectors are always written as row vectors.

Definition 1 Let \( q \) be a prime power and let \( n, m, s \) be natural numbers. Let \( C_1, \ldots, C_s \) be \( n \times m \) matrices over the finite field \( \mathbb{F}_q \) of order \( q \). We construct \( q^m \) points in \([0,1]^s\) in the following way: For \( 0 \leq h < q^m \) let \( h = h_0 + h_1 q + \cdots + h_{m-1} q^{m-1} \) be the base \( q \) representation of \( h \). Consider an arbitrary but fixed bijection \( \eta : \{0,1,\ldots,q-1\} \to \mathbb{F}_q \) where
η(0) is the zero element in \( \mathbb{F}_q \). Identify \( h \) with the vector \( \mathbf{h} := (\eta(h_0), \ldots, \eta(h_{m-1})) \in \mathbb{F}_q^m \). For \( 1 \leq j \leq s \), we multiply the matrix \( C_j \) by \( \mathbf{h} \), i.e.,

\[
C_j \cdot \mathbf{h}^\top =: (y_{j,1}(h), \ldots, y_{j,n}(h)) \in \mathbb{F}_q,
\]

and set

\[
x_h^{(j)} := \frac{\eta^{-1}(y_{j,1}(h))}{q} + \cdots + \frac{\eta^{-1}(y_{j,n}(h))}{q^n}.
\]

Finally, set \( \mathbf{x}_h := \left(x_h^{(1)}, \ldots, x_h^{(s)}\right) \). The point set consisting of the points \( \mathbf{x}_0, \ldots, \mathbf{x}_{q^m-1} \) is called a digital net over \( \mathbb{F}_q \). The matrices \( C_1, \ldots, C_s \) are called the generating matrices of the digital net.

As it can be seen from Definition 1, the properties of the points of a digital net (such as, e.g., their distribution in the unit cube) are determined by properties of the generating matrices \( C_1, \ldots, C_s \). These properties are, in the currently most general form of digital nets as introduced in [4], described by additional parameters \( t, \alpha, \beta \), which is why those nets are referred to as \((t, \alpha, \beta, n \times m, s)\)-nets. The exact role of the parameters \( t, \alpha \) and \( \beta \) is stated in the following definition.

**Definition 2** Let \( n, m, \alpha \geq 1 \) be natural numbers, let \( 0 < \beta \leq \min(1, \alpha m/n) \) be a real number such that \( \beta n \) is an integer. Let \( \mathbb{F}_q \) be the finite field of prime power order \( q \) and let \( C_1, \ldots, C_s \in \mathbb{F}^{n\times m}_q \) with \( C_j = (\overline{c}_{1,j}, \ldots, \overline{c}_{s,j})^\top \). The digital net with generating matrices \( C_1, \ldots, C_s \) is called a digital \((t, \alpha, \beta, n \times m, s)\)-net for a natural number \( t \), \( 0 \leq t \leq \beta n \), if the following condition is satisfied. For each choice of \( 1 \leq i_{j,0} < \cdots < i_{j,1} \leq n \), where \( \nu_j \geq 0 \) for \( j = 1, \ldots, s \), with

\[
i_{1,1} + \cdots + i_{1,\min(\nu_1, \alpha)} + \cdots + i_{s,1} + \cdots + i_{s,\min(\nu_s, \alpha)} \leq \beta n - t
\]

the vectors

\[
\overline{c}_{i_{1,1}, \nu_1}, \ldots, \overline{c}_{i_{1,1}, 1}, \ldots, \overline{c}_{s,i_{s,\nu_s}}, \ldots, \overline{c}_{s,i_{s,1}}
\]

are linearly independent over \( \mathbb{F}_q \).

If \( t \) is the smallest non-negative integer such that the digital net generated by \( C_1, \ldots, C_s \) is a digital \((t, \alpha, \beta, n \times m, s)\)-net, then we call the digital net a strict digital \((t, \alpha, \beta, n \times m, s)\)-net.

**Remark 1** Note that Definition 2 implies that \( t \) must be chosen such that \( \nu_1 + \cdots + \nu_s \leq m \) holds whenever (1) is satisfied. (Note that \( \nu_j \leq i_{j,1} \).)

**Remark 2** Without loss of generality we added the condition that \( \beta \leq 1 \) in Definition 2. Note that there is some redundancy in Definition 2. One could view the value \( \beta n - t \) as the strength of the digital net, which is the value which matters in Definition 2. Through which values of \( \beta \) and \( t \) a particular strength was obtained does not have any influence, i.e., a digital \((t, \alpha, \beta, n \times m, s)\)-net has the same properties as a digital \((t', \alpha, \beta', n \times m, s)\)-net, as long as \( \beta n - t = \beta' n - t' \) (see also Theorem 2 below). In view of [4, Remark 5.3] we can therefore assume without loss of generality that \( \beta \leq 1 \).

To understand why this redundancy is needed one needs to consider digital sequences. As in the classical case, we base the definition of digital sequences on the definition of digital nets, i.e., each suitable subset of the digital sequence has to be a digital \((t, \alpha, \beta, n \times m, s)\)-net. When one considers digital sequences, the redundancy of \( \beta \) and \( t \) then disappears, see [4] for the definition of such digital sequences.
The definition of classical digital \((t, m, s)\)-nets is obtained by choosing \(\alpha = \beta = 1\) and \(m = n\) in Definition 2.

**Remark 3** As already indicated in Remark 2, the value of the difference \(\beta n - t\) is crucial for the quality of a digital net. This is why \(\beta n - t\) (which simplifies to \(m - t\) in the case of classical digital nets) is referred to as strength of the digital net. Generally speaking, it is desirable to obtain digital nets with strength as large as possible, i.e., one is interested in constructing nets with low \(t\)-value. However, due to the involved interdependence of the parameters of a digital net, there are many combinatorial restrictions on the possible values of the strength of a digital net. The question of which strength of a digital net can be achieved or not is in general non-trivial (cf. [13]).

To illustrate the usefulness of digital \((t, \alpha, \beta, n \times m, s)\)-nets for numerical integration, we state the following result:

**Theorem 1** Let \(\{x_0, \ldots, x_{q^{m-1}}\}\) be a digital \((t, \alpha, \beta, n \times m, s)\)-net over the finite field \(\mathbb{F}_q\). Let \(f : [0, 1]^s \to \mathbb{R}\) have mixed partial derivatives up to order \(\alpha \geq 1\) in each variable which are square integrable. Then

\[
\left| \int_{[0,1]^s} f(x) \, dx - \frac{1}{q^m} \sum_{h=0}^{q^m-1} f(x_h) \right| = O \left( q^{-\beta n - t} (\beta n - t)^{\alpha s} \right).
\]

For \(\alpha = 1\) this is a classical result, see for example [7], and for \(\alpha > 1\) see [4]. Hence it is important to have explicit constructions of digital nets with a large value of \(\beta n - t\).

In a series of papers, see for example [1, 9, 11], so-called propagation rules for digital \((t, m, s)\)-nets were introduced, which allow one to construct new digital nets from known ones and thereby improve on the parameters, in particular on the strength, of those nets. That such constructions are very useful can be seen in [13], where the best known parameters of classical \((t, m, s)\)-nets are listed. Even though many propagation rules have been studied for the case of classical digital nets (see again [13]), there has, so far, been no systematic approach to propagation rules for the generalized digital \((t, \alpha, \beta, n \times m, s)\)-nets introduced in [4]. It is the aim of this paper to study such rules for the generalized digital nets in greater detail, and thereby find new ways of explicitly constructing digital nets of high quality (see Section 4 for numerical results).

Some simple propagation rules for generalized digital nets were already stated in [4], for a proof see [3, Theorem 3.3]. For completeness we repeat them in the following theorem, and also include some further trivial propagation rules.

**Theorem 2 (Propagation Rules I–VI)** Let \(P\) be a digital \((t, \alpha, \beta, n \times m, s)\)-net over \(\mathbb{F}_q\) with generating matrices \(C_1, \ldots, C_s \in \mathbb{F}_q^{n \times m}\). Then we have the following:

(i) \(P\) is a digital \((t', \alpha', \beta', n \times m, s)\)-net for all \(0 < \beta' \leq \min(1, \alpha m/n)\) and all \(t' \leq \beta' n - \beta'n - t\).

(ii) \(P\) is a digital \((t', \alpha', \beta', n \times m, s)\)-net for all \(1 \leq \alpha' \leq n\), where \(\beta' = \beta \min(1, \alpha'/\alpha)\) and \(t' = \lceil t \min(1, \alpha'/\alpha) \rceil\).

(iii) Let \(1 \leq n' \leq n\). Then the matrices \(C_1^{(n')}, \ldots, C_s^{(n')}, \) where \(C_j^{(n')}\) consists of the first \(n'\) rows of \(C_j\), generate a digital \((t', \alpha, \beta, n' \times m, s)\)-net, where \(t' = \max(t - \beta(n - n'), 0)\).
(iv) Let \( n' \geq n \). Then the generating matrices \( C_1^{(n')}, \ldots, C_s^{(n')} \), where the first \( n \) rows of \( C_j^{(n')} \) are the same as those of \( C_j \) and the remaining \( n' - n \) rows are \( 0 = (0, \ldots, 0) \in \mathbb{F}_q^n \), generate a digital \((t, \alpha, \beta', n' \times m, s')\)-net, where \( \beta' = \beta n/n' \).

(v) Let \( 1 \leq s' \leq s \) and \( u \subseteq \{1, \ldots, s\} \) be a subset of cardinality \( s' \). Then the set of generating matrices \( \{C_j : j \in u\} \), generate a digital \((t, \alpha, \beta, n \times m, s')\)-net.

(vi) For \( 1 \leq j \leq s \), let \( C'_j \in \mathbb{F}_{q}^n \times (m+v) \) be the matrix obtained by augmenting \( C_j \) with \( v \) columns of \( 0^\top = (0, \ldots, 0)^\top \in \mathbb{F}_q^n \). Then \( C'_1, \ldots, C'_s \) generate a digital \((t, \alpha, \beta, n \times (m+v), s')\)-net.

In this paper, we discuss further (non-trivial) propagation rules. In some cases it is convenient to view those propagation rules from the dual space of the digital net, which is why we generalize the duality theory of [10] to the digital nets of Definition 2 in Section 2. Using this theory, we then establish generalizations of the propagation rules which are known for digital \((t, m, s)\)-nets. Here we introduce generalizations of the following propagation rules: The direct product of digital nets (see e.g. [8]), the \((u, u+v)\)-construction [1], the matrix-product construction [9], three different base change propagation rules [11, 12, 13] and the construction of higher order nets of [4].

Throughout the paper, we assume that \( q \) is a prime power and \( \mathbb{F}_q \) is the finite field of order \( q \). Once again we remark that vectors \( \mathbf{c} \in \mathbb{F}_q^m \) will always denote row vectors.

## 2 Duality Theory

In this section we generalize the duality theory introduced in [10] to digital \((t, \alpha, \beta, n \times m, s)\)-nets. Given generating matrices \( C_1, \ldots, C_s \) of a generalized digital net, let

\[
C = (C_1^\top | \cdots | C_s^\top) \in \mathbb{F}_q^{m \times sn}.
\]

The row space of \( C \), denoted by \( \mathcal{C} \), is a linear subspace of \( \mathbb{F}_q^{sn} \). We define the dual space \( \mathcal{N} \) of \( \mathcal{C} \) as the null space of \( C \).

Let \( \alpha \in \mathbb{N} \). For \( \mathbf{a} \in \mathbb{F}_q^n \) let \( \mu_\alpha(\mathbf{0}) = 0 \) and for \( \mathbf{a} = (a_1, \ldots, a_n) \), where the only non-zero elements are \( a_{i_1}, a_{i_2}, \ldots, a_{i_v} \), with \( n \geq i_1 > i_2 > \cdots > i_v \geq 1 \), let \( \mu_\alpha(\mathbf{a}) = t_1 + \cdots + t_{\min(\alpha, v)} \). For vectors \( \mathbf{A} = (\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(s)}) \in \mathbb{F}_q^{sn} \), with \( \mathbf{a}^{(i)} \in \mathbb{F}_q^n \) for \( 1 \leq i \leq s \), we define

\[
\mu_{\alpha, n}(\mathbf{A}) = \sum_{i=1}^s \mu_\alpha(\mathbf{a}^{(i)}).
\]

**Remark 4** For \( \alpha = 1 \) we obtain the definition of the quantity \( V_m \) in [10].

**Definition 3** For any non-zero linear subspace \( \mathcal{N} \) of \( \mathbb{F}_q^{sn} \) we define the minimum distance

\[
\delta_{\alpha, n}(\mathcal{N}) = \min_{\mathbf{A} \in \mathcal{N} \setminus \{\mathbf{0}\}} \mu_{\alpha, n}(\mathbf{A}).
\]

We always have \( \delta_{\alpha, n}(\mathcal{N}) \geq 1 \) and \( \delta_{\alpha, n}(\mathcal{N}) \geq \delta_{\alpha', n}(\mathcal{N}) \) for \( \alpha \geq \alpha' \geq 1 \).

We generalize [10, Proposition 1], which itself is a generalization of the Singleton bound from coding theory. The proof can be obtained along the same lines as the proof of [10, Proposition 1]. We put \( (x)_+ = \max(x, 0) \).
Proposition 1 Let \( N \) be a non-zero linear subspace of \( \mathbb{F}^{sn}_q \) with \( h = \dim(N) - 1 = rn + u \), where \( 0 \leq u < n \) and \( 0 \leq r < s \). Then we have

\[
\delta_{\alpha,n}(N) \leq (s-r-1)[n+(n-1)+(n-2)_+ + \cdots + (n-\alpha+1)_+] \\
+ (n-u)+(n-u-1)+(n-u-2)_+ + \cdots + (n-u-\alpha+1)_+.
\]

Proof. We have \( h \geq 0 \). Let \( \pi : N \to \mathbb{F}_q^{h+1} \) be the linear transformation which maps \( A \in N \) to the \((h+1)\)-tuple of the last \( h+1 \) coordinates of \( A \). If \( \pi \) is surjective, then there exists a non-zero \( A_1 \in N \) with \( \pi(A_1) = (1,0,\ldots,0) \in \mathbb{F}_q^{h+1} \), i.e., the last \( h \) coordinates of \( A_1 \) are 0. Then

\[
\mu_{\alpha,n}(A_1) \leq (s-r-1)[n+(n-1)+(n-2)_+ + \cdots + (n-\alpha+1)_+] \\
+ (n-u)+(n-u-1)+(n-u-2)_+ + \cdots + (n-u-\alpha+1)_+.
\]

If \( \pi \) is not surjective, then for any \( A_2 \) in the kernel of \( \pi \) we have

\[
\mu_{\alpha,n}(A_2) < (s-r-1)[n+(n-1)+(n-2)_+ + \cdots + (n-\alpha+1)_+] \\
+ (n-u)+(n-u-1)+(n-u-2)_+ + \cdots + (n-u-\alpha+1)_+.
\]

In both cases we get the result of the proposition. \( \square \)

Remark 5 Putting \( \alpha = 1 \) in the proposition above yields [10, Proposition 1].

We can also obtain the analogue to [10, Theorem 1], which was already stated in [4, Remark 4.4].

Theorem 3 The matrices \( C_1,\ldots,C_s \in \mathbb{F}^{n \times m}_q \) generate a digital \((t,\alpha,\beta,n \times m,s)\)-net over \( \mathbb{F}_q \) if and only if

\[
\delta_{\alpha,n}(N) \geq \beta n - t + 1,
\]

where \( N \) is the dual space of the row space \( \mathcal{C} \). If \( C_1,\ldots,C_s \) generate a strict digital \((t,\alpha,\beta,n \times m,s)\)-net over \( \mathbb{F}_q \), then

\[
\delta_{\alpha,n}(N) = \beta n - t + 1.
\]

We also have the following result.

Proposition 2 We have

\[
\dim(\mathcal{C}) \leq m \quad \text{and} \quad \dim(N) \geq sn - m.
\]

Proof. The bound on the dimension of \( \mathcal{C} \) follows as \( \mathcal{C} \) is the row space of a matrix with \( m \) rows. The second inequality follows as \( N \) is the null space of \( \mathcal{C} \) and therefore \( \dim(N) = sn - \dim(\mathcal{C}) \). \( \square \)

3 Propagation Rules

In this section we introduce several propagation rules for digital \((t,\alpha,\beta,n \times m,s)\)-nets. Analogues for digital \((t,m,s)\)-nets exist already in the literature (those cases are also covered as special cases of our results).
3.1 Direct Product of Two Nets

As in the classical case (see, e.g., [8]), a digital \((t, \alpha, \beta, n \times m, s)\)-net can be constructed by forming the direct product of two smaller nets.

To be more precise, let \(q\) be a prime power, let \(P_1\) be a digital \((t_1, \alpha_1, \beta_1, n_1 \times m_1, s_1)\)-net over \(\mathbb{F}_q\) and \(P_2\) a digital \((t_2, \alpha_2, \beta_2, n_2 \times m_2, s_2)\)-net over the same field. We denote the points of \(P_1\) by \(x_{0,1}, \ldots, x_{q^{n_1-1}}, 1\) and the points of \(P_2\) by \(x_{0,2}, \ldots, x_{q^{n_2-1}}\). Furthermore, we denote the generating matrices of \(P_1\) and \(P_2\) by \(C_{1,1}, \ldots, C_{s_1,1}\) and \(C_{1,2}, \ldots, C_{s_2,2}\), respectively. Based on \(P_1\) and \(P_2\), we form a new digital \((t, \alpha, \beta, n \times m, s)\)-net \(P\) over \(\mathbb{F}_q\), where \(n = n_1 + n_2\), \(m = m_1 + m_2\), and \(s = s_1 + s_2\). The points of \(P\) are defined to be the direct product of the points of \(P_1\) and \(P_2\), i.e., \(P\) is the collection of the \(b^m\) points

\[(x_{i_1,1}, x_{i_2,2}), \quad 0 \leq i_1 \leq q^{n_1} - 1, 0 \leq i_2 \leq q^{n_2} - 1.\]

For the generating matrices \(D_1, \ldots, D_s\) of \(P\), this means that

\[D_j = \begin{pmatrix} C_{j,1} & 0^{n_1 \times m_2} \\ 0^{n_2 \times m_1} & 0^{n_2 \times m_2} \end{pmatrix}, \quad 1 \leq j \leq s_1,\]

and

\[D_j = \begin{pmatrix} 0^{n_2 \times m_1} & C_{j-s_1,2} \\ 0^{n_1 \times m_1} & 0^{n_1 \times m_2} \end{pmatrix}, \quad s_1 + 1 \leq j \leq s,\]

where \(0^{k \times l}\) denotes a \(k \times l\) matrix consisting only of zeros. In the following, we denote the \(i\)-th row of the matrix \(D_j\) by \(d_{j,i}\) for \(1 \leq j \leq s\).

We have the following result.

**Theorem 4 (Propagation Rule VII)** Let \(q\) be a prime power, let \(P_1\) be a digital \((t_1, \alpha_1, \beta_1, n_1 \times m_1, s_1)\)-net over \(\mathbb{F}_q\) and \(P_2\) a digital \((t_2, \alpha_2, \beta_2, n_2 \times m_2, s_2)\)-net over the same field. Then \(P\) is a digital \((t, \alpha, \beta, n \times m, s)\)-net over \(\mathbb{F}_q\), where \(n = n_1 + n_2\), \(m = m_1 + m_2\), \(s = s_1 + s_2\), and

\[\alpha = \max\{\alpha_1, \alpha_2\}, \quad \beta = \min\{\beta_1, \beta_2\}, \quad t \leq \max\{\beta_1 n_1 + t_2, \beta_2 n_2 + t_1\}.\]

**Proof.** It is easily verified that \(0 \leq \beta \leq \min(1, \alpha M/n)\). We need to check that \(t\), as given above, satisfies the necessary conditions such that \(P\) is indeed a \((t, \alpha, \beta, n \times m, s)\)-net. Let \(\nu_1, \ldots, \nu_s \geq 0\) and, for \(1 \leq j \leq s\), let \(1 \leq i_{j,\nu_j} < i_{j,\nu_j-1} < \cdots < i_{j,1} \leq n\), with

\[i_{1,1} + \cdots + i_{1,\min\{\nu_1, \alpha\}} + \cdots + i_{s,1} + \cdots + i_{s,\min\{\nu_s, \alpha\}} \leq \beta n - t. \tag{3}\]

Note that \(\beta n - t\) does neither exceed \(\beta_1 n_1 - t_1\) nor \(\beta_2 n_2 - t_2\). Thus, (3) implies

\[i_{1,1} + \cdots + i_{1,\min\{\nu_1, \alpha\}} + \cdots + i_{s,1} + \cdots + i_{s,\min\{\nu_s, \alpha\}} \leq \beta_1 n_1 - t_1,\]

\[i_{s_1+1,1} + \cdots + i_{s_1+1,\min\{\nu_{s_1+1}, \alpha\}} + \cdots + i_{s,1} + \cdots + i_{s,\min\{\nu_s, \alpha\}} \leq \beta_2 n_2 - t_2,\]

and, since \(\beta_1, \beta_2 \leq 1\),

\[i_{j,1} \leq n_1, \quad 1 \leq j \leq s_1, \quad \text{and} \quad i_{j,1} \leq n_2, \quad s_1 + 1 \leq j \leq s.\]

As a consequence, we have that the row vectors \(d_{j,i_{j,\nu_j}}, \ldots, d_{j,i_{j,1}}\) are rows of the matrix

\[
\begin{pmatrix} C_{j,1} & 0^{n_1 \times m_2} \\
0^{n_2 \times m_1} & 0^{n_2 \times m_2} \end{pmatrix}
\]
for each \( j \in \{1, \ldots, s_1\} \). Similarly, the row vectors \( d_{j,j_2,j_2}, \ldots, d_{j,j_1,1} \) are rows of the matrix
\[
\begin{pmatrix}
0_{n_2 \times m_1} & C_{j-s_1,2}
\end{pmatrix}
\]
for each \( j \in \{s_1 + 1, \ldots, s\} \), respectively.

Due to the assumptions made on \( P_1 \) and \( P_2 \), it thus follows that the row vectors
\[
d_{1,i_1,i_1}, \ldots, d_{i_1,i_1,1}, \ldots, d_{s,i_s,i_s}, \ldots, d_{s,i_s,1}
\]
are linearly independent, which completes the proof.

\( \square \)

**Remark 6** Note that for \( i = 1, 2 \) we always have \( \beta_i n_i \leq \alpha_i m_i \), and as \( \beta n - t \leq \beta_i n_i - t_i \), \( i = 1, 2 \), we obtain \( \beta n - t \leq \alpha_i m_i \). In order to obtain the best rate of convergence of the integration error, we require \( \beta n \) to be of order \( \alpha \alpha m \) (see Theorem 1 or [4, Corollary 5.5]). Note that we view \( \beta \) and \( t \) as functions of \( \alpha \) (see [4, Remark 4.5]). Thus, to achieve such a convergence rate one should find values \( t_1, t_2, \beta_1, \beta_2 \) for \( \alpha_1 = \alpha_2 \).

### 3.2 The \((u, u + v)\)-Construction

In the classical case of digital \((t, m, s)\)-nets there is a construction stemming from coding theory called the \((u, u + v)\)-construction (see, e.g., [1]). We now show that a similar construction is possible in the generalized case. However, we do not outline the \((u, u + v)\)-construction in its coding theoretic context, but show the result by making use of the generating matrices of the digital nets.

Let again \( P_1 \) be a digital \((t_1, \alpha_1, \beta_1, n_1 \times m_1, s_1)\)-net over \( \mathbb{F}_q \), with generating matrices \( C_{1,1}, \ldots, C_{s_1,1} \), and let \( P_2 \) be a digital \((t_2, \alpha_2, \beta_2, n_2 \times m_2, s_2)\)-net over \( \mathbb{F}_q \) with generating matrices \( C_{1,2}, \ldots, C_{s_2,2} \). We assume that \( s_1 \leq s_2 \). From these two digital nets we form a new digital \((t, \alpha, \beta, n \times m, s)\)-net over \( \mathbb{F}_q \), where \( n = n_1 + n_2, m = m_1 + m_2 \), and \( s = s_1 + s_2 \), in the following way: Let

\[
k := \min\{2\beta_1 n_1 - 2t_1 + 1, \beta_2 n_2 - t_2\}
\]

and let \( P \) be the digital net generated by the matrices \( D_1, \ldots, D_s \), with

\[
D_j = \begin{pmatrix}
C_{j,1} & -(C_{j,2})^{k \times m_2} \\
0_{n_2 \times m_1} & 0^{(n-k) \times m_2}
\end{pmatrix}, \quad 1 \leq j \leq s_1
\]

and

\[
D_j = \begin{pmatrix}
0_{n_2 \times m_1} & C_{j-s_1,2} \\
0_{n_1 \times m_1} & 0^{n_1 \times m_2}
\end{pmatrix}, \quad s_1 + 1 \leq j \leq s,
\]

where \((C_{j,2})^{k \times m_2}\) denotes the matrix that consists of the first \( k \) rows of \( C_{j,2} \) and \(-(C_{j,2})^{k \times m_2}\) denotes the additive inverse in \( \mathbb{F}_q \) of the matrix \((C_{j,2})^{k \times m_2}\).

The following propagation rule generalizes the \((u, u + v)\)-construction from [1].

**Theorem 5 (Propagation Rule VIII)** Let \( q \) be a prime power, let \( P_1 \) be a digital \((t_1, \alpha_1, \beta_1, n_1 \times m_1, s_1)\)-net over \( \mathbb{F}_q \) and \( P_2 \) a digital \((t_2, \alpha_2, \beta_2, n_2 \times m_2, s_2)\)-net over the same field. Furthermore, let \( P \) be defined as above. Then \( P \) is a digital \((t, \alpha, \beta, n \times m, s)\)-net over \( \mathbb{F}_q \), where \( n = n_1 + n_2, m = m_1 + m_2, s = s_1 + s_2, \) and

\[
\alpha = \max\{\alpha_1, \alpha_2\}, \quad \beta = \min\{\beta_1, \beta_2\}, \quad t = \beta n - k.
\]
Remark 7 Similar to Remark 6, one should use \( \alpha_1 = \alpha_2 \) in Theorem 5 in order to be able to obtain \( \beta n \) to be of order \( \alpha n \).

We omit the proof of the last theorem, as the \((u, u + v)\)-construction is a special case of the matrix-product construction, which we consider in the next section.

### 3.3 The matrix-product construction

The matrix-product construction for classical digital nets was introduced in [9], which itself is a generalization of the matrix-product construction of codes in [2]. The \((u, u + v)\)-construction considered above is a special case thereof. In the following we introduce the construction principle, which works in exactly the same way as the construction introduced in [9] for \((d, k, m, s)\)-systems, and then provide a bound on the quality of digital nets obtained this way. First we introduce some notation and definitions, where we follow [9].

Let us first introduce matrices which are non-singular by column (NSC matrices) [2].

Let \( A \) be an \( M \times M \) matrix over a finite field \( \mathbb{F}_q \). For \( 1 \leq l \leq M \), let \( A_l \) denote the matrix which consists of the first \( l \) rows of \( A \). For \( 1 \leq k_1 < \cdots < k_l \leq M \), let \( A(k_1, \ldots, k_l) \) denote the \( l \times l \) matrix consisting of the columns \( k_1, \ldots, k_l \) of \( A_l \).

**Definition 4** We call an \( M \times M \) matrix \( A \) defined over a finite field \( \mathbb{F}_q \) non-singular by columns (NSC) if \( A(k_1, \ldots, k_l) \) is non-singular for each \( 1 \leq l \leq M \) and \( 1 \leq k_1 < \cdots < k_l \leq M \).

Recall that an \( M \times M \) matrix \( A = (A_{k,l}) \) is upper triangular if \( A_{k,l} = 0 \) for all \( 1 \leq l < k \leq M \).

**Remark 8** As noted in [9], an \( M \times M \) NSC matrix over \( \mathbb{F}_q \) exists if and only if \( 1 \leq M \leq q \), see [2, Section 3]. For any integer \( 1 \leq M \leq q \), an explicit \( M \times M \) upper triangular NSC matrix over \( \mathbb{F}_q \) is given in [2, Section 5.2].

For the matrix-product construction in its general form, another definition is needed.

**Definition 5** Let \( 1 \leq r_1 \leq \cdots \leq r_M \) be integers and \( V_1 \subseteq \mathbb{F}_{q_{r_1}}, \ldots, V_M \subseteq \mathbb{F}_{q_{r_M}} \) be vector spaces over \( \mathbb{F}_q \). Let \( r = r_M \) and for each \( 1 \leq l \leq M \) and any \( \mathbf{v}_l \in V_l \), let \( \mathbf{v}_l \in \mathbb{F}_{q^r} \) be the vector obtained from \( \mathbf{v}_l \) by appending zero entries if \( r_l < r \). We call an \( M \times M \) matrix \( A \) over \( \mathbb{F}_q \) compatible with \( (V_1, \ldots, V_M) \), if for any vectors \( \mathbf{v}_1 \in V_1, \ldots, \mathbf{v}_M \in V_M \) and \( \tilde{\mathbf{u}}_1, \ldots, \tilde{\mathbf{u}}_M \in \mathbb{F}_q^r \) with

\[
[\tilde{\mathbf{u}}_1 \ldots \tilde{\mathbf{u}}_M] = [\mathbf{v}_1^\top \ldots \mathbf{v}_M^\top] \cdot A
\]

and

\[
\tilde{\mathbf{u}}_l = [\tilde{u}_{1,l} \ldots \tilde{u}_{r,l}] \in \mathbb{F}_q^{r_l} \quad \text{for} \quad 1 \leq l \leq M,
\]

we have \( \tilde{u}_{k,l} = 0 \) for each \( 1 \leq l \leq M \) and \( r_l < k \leq r \).

The following remark and lemma are from [9].

**Remark 9** For any integers \( 1 \leq r_1 \leq \cdots \leq r_M \), if \( A \) is an \( M \times M \) matrix over \( \mathbb{F}_q \) compatible with \( (\mathbb{F}_{q_{r_1}}, \ldots, \mathbb{F}_{q_{r_M}}) \), then \( A \) is compatible with \( (V_1, \ldots, V_M) \) for any vector spaces \( V_1 \subseteq \mathbb{F}_{q_{r_1}}, \ldots, V_M \subseteq \mathbb{F}_{q_{r_M}} \) over \( \mathbb{F}_q \).
Lemma 1 Let \( A \) be an \( M \times M \) upper triangular matrix over \( \mathbb{F}_q \). For any integers \( 1 \leq r_1 \leq \cdots \leq r_M \), \( A \) is compatible with \( (\mathbb{F}_q^{r_1}, \ldots, \mathbb{F}_q^{r_M}) \).

We are now ready to introduce the matrix-product construction. Assume we are given digital \((t_k, \alpha, \beta_k, n_k \times m_k, s_k)\)-nets over \( \mathbb{F}_q \) with generating matrices \( C_{1,k}, \ldots, C_{s_k,k} \), \( 1 \leq k \leq M \), where we assume that \( 1 \leq s_1 \leq \cdots \leq s_M \). Note that we now use the same value of \( \alpha \) for all \( M \) digital nets, i.e., we assume that \( t_k \) and \( \beta_k \) are known for the same given value of \( \alpha \) for \( k = 1, \ldots, M \). By adding zeroes at the appropriate places in the respective generating matrices we can assume that \( n_1 = \cdots = n_M = n \), i.e., we replace each \( C_{j,k} \) with \( C'_{j,k} \) where the rows \( n_k + 1, \ldots, n \) are \((0, \ldots, 0)\) and the first \( n_k \) rows of \( C_{j,k} \) and \( C'_{j,k} \) are the same for \( j = 1, \ldots, s_k \).

As in Section 2, for \( 1 \leq k \leq M \) we form the matrices

\[
C_k = ((C'_{1,k})^\top | \cdots | (C'_{s_k,k})^\top).
\]

The row space of \( C_k \) is denoted by \( \mathcal{C}_k \subseteq \mathbb{F}_q^{n_{s_k}} \) and the dual space of \( C_k \) is denoted by \( \mathcal{C}_k^\perp \subseteq \mathbb{F}_q^{n_{s_k}} \).

Put \( s = s_M \) and for each \( k = 1, \ldots, M \) and \( a_k \in \mathcal{C}_k \), let \( \bar{a}_k \in \mathbb{F}_q^{n_s} \) be the vector obtained from \( a_k \in \mathbb{F}_q^{n_{s_k}} \) by appending enough zeroes, that is,

\[
\bar{a}_k^\top = \begin{pmatrix} a_k^\top \\ 0 \end{pmatrix} = \begin{pmatrix} a_{1,k}^\top \\ \vdots \\ a_{s_k,k}^\top \\ 0 \end{pmatrix},
\]

where \( a_{j,k} \in \mathbb{F}_q^m \) for \( 1 \leq k \leq M \) and \( 1 \leq j \leq s_k \).

For the remainder of this section we will assume that \( A \) is an \( M \times M \) NSC matrix over \( \mathbb{F}_q \) which is compatible with \( (C_1^\perp, \ldots, C_M^\perp) \) (this of course implies that \( M \leq q \)). For example, we can choose an upper triangular NSC matrix as \( A \).

Let

\[
\mathcal{M} := \{ (a_1^\top a_2^\top \cdots a_M^\top) \cdot A : a_k \in \mathcal{C}_k^\perp \text{ for } 1 \leq k \leq M \},
\]

i.e., \( \mathcal{M} \) is a linear space of \((ns) \times M \) matrices over \( \mathbb{F}_q \). In the next step we define an \( \mathbb{F}_q \)-linear mapping

\[
\phi : \mathcal{M} \to \mathbb{F}_q^{n(s_1 + \cdots + s_M)}.
\]

Let

\[
\bar{C} = (\bar{c}_1^\top \bar{c}_2^\top \cdots \bar{c}_M^\top) \in \mathcal{M}
\]

be a matrix in \( \mathcal{M} \), where

\[
\bar{c}_k^\top = \begin{pmatrix} \bar{c}_{1,k}^\top \\ \bar{c}_{2,k}^\top \\ \vdots \\ \bar{c}_{s_k,k}^\top \\ 0 \end{pmatrix}
\]

and \( \bar{c}_{j,k} \in \mathbb{F}_q^n \) for \( 1 \leq k \leq M \) and \( 1 \leq j \leq s_k \). Since \( A \) is invertible, there exist uniquely determined vectors \( a_1 \in \mathcal{C}_1^\perp, \ldots, a_M \in \mathcal{C}_M^\perp \), such that

\[
(\bar{c}_1^\top \cdots \bar{c}_M^\top) = (\bar{a}_1^\top \cdots \bar{a}_M^\top) \cdot A.
\]
Note that for $1 \leq k \leq M$ we have

$$\bar{a}_k^\top = \begin{pmatrix} \bar{a}_{1,k}^\top \\ \vdots \\ \bar{a}_{s,k}^\top \end{pmatrix},$$

where $\bar{a}_{j,k} = a_{j,k} \in \mathbb{F}_q^n$ for $1 \leq j \leq s_k$ and $\bar{a}_{j,k} = 0 \in \mathbb{F}_q^n$ for $s_k < j \leq s$. By (4), we have

$$\bar{c}_{j,k}^\top = \sum_{v=1}^{M} a_{j,v}^\top A_{v,k}$$

(5)

for each $1 \leq k \leq M$ and $1 \leq j \leq s$. For any $1 \leq k \leq M$, let $c_k \in \mathbb{F}_q^{ns_k}$ be the vector obtained by taking the first $s_k$ blocks of $\bar{c}_k \in \mathbb{F}_q^{ns}$, that is,

$$c_k^\top = \begin{pmatrix} \bar{c}_{1,k}^\top \\ \vdots \\ \bar{c}_{s_k,k}^\top \end{pmatrix},$$

Since $A$ is compatible with $(C_1^\perp, \ldots, C_M^\perp)$, we have

$$\bar{c}_{j,k} = 0 \in \mathbb{F}_q^n$$

for any $1 \leq k \leq M$ and $s_k < j \leq s$. Let $C \in \mathbb{F}_q^{n(s_1+\cdots+s_M)}$ be the vector

$$C = (c_1 c_2 \ldots c_M).$$

We define the $\mathbb{F}_q$-linear mapping $\phi : \mathcal{M} \to \mathbb{F}_q^{n(s_1+\cdots+s_M)}$ by $\phi(C) = C$.

Let $\mathcal{N} = \phi(\mathcal{M})$. Let $C \in (c_1 \ldots c_M) \in \mathcal{N}$ be a vector, where for each $1 \leq k \leq M$ we have $c_k \in \mathbb{F}_q^{ns_k}$ with

$$c_k^\top = \begin{pmatrix} c_{1,k}^\top \\ \vdots \\ c_{s_k,k}^\top \end{pmatrix},$$

and $c_{j,k} \in \mathbb{F}_q^n$ for $1 \leq j \leq s_k$. The set $\mathcal{N}$ is now the dual space of a digital $(t, \alpha, \beta, n \times m, s)$-net, where $s = s_1 + \cdots + s_M$, $m = m_1 + \cdots + m_M$, and $n = \max_{1 \leq k \leq M} n_k$ (one could also set $n = n_1 + \cdots + n_M$ by appending zeroes at the last rows of the generating matrices as was done with $C'_{j,k}$ after Remark 8).

We now investigate the quality of the digital nets obtained via the matrix-product construction, i.e., we find a lower bound on $\delta_{\alpha,n}(\mathcal{N})$. We have

$$\mu_{\alpha,n}(C) = \sum_{k=1}^{M} \mu_{\alpha,n}(c_k) = \sum_{k=1}^{M} \sum_{j=1}^{s_k} \mu_{\alpha}(c_{j,k}).$$

We have $C = (c_1 \ldots c_M) \in \mathbb{F}_q^{n(s_1+\cdots+s_M)}$ and assume that $C \neq 0$. By the definition of $C$, there are vectors $a_1 \in C_1^\perp, \ldots, a_M \in C_M^\perp$ such that

$$(c_1^\top \ldots c_M^\top) = (a_1^\top \ldots a_M^\top) \cdot A.$$
Let $l$ be the largest integer such that $a_l \neq 0$ (this exists as $C \neq 0$). Note that

$$a_l^\top = \begin{pmatrix} a_{1,l}^\top \\ \vdots \\ a_{s,l}^\top \end{pmatrix}$$

and $\mu_{\alpha,n}(a_l) = \sum_{j=1}^{s_l} \mu_{\alpha}(a_{j,l})$. Let $\{j_1, \ldots, j_u\}$ be the largest subset of $\{1, \ldots, s_l\}$ such that $a_{j,l} \neq 0$ for all $j \in \{j_1, \ldots, j_u\}$. By the definition of $l$ we have $u \geq 1$. Moreover, we note that $\mu_{\alpha,n}(a_l) = \mu_{\alpha}(a_{j_1,l}) + \cdots + \mu_{\alpha}(a_{j_u,l})$.

The following lemma is a generalization of [9, Lemma 4.1].

**Lemma 2** Under the notation and assumptions as above, for each $j \in \{j_1, \ldots, j_u\}$ we have

$$\mu_{\alpha}(c_{j,1}) + \cdots + \mu_{\alpha}(c_{j,M}) \geq (M - l + 1)\mu_{\alpha}(a_{j,l}).$$

**Proof.** Let $j \in \{j_1, \ldots, j_u\}$, and let $\tilde{a}_{j,l} = (a_{j,l,1} \ldots a_{j,l,n})$. Further let $n \geq i_{j,l,1} > \cdots > i_{j,l,v} \geq 1$ be such that $a_{j,l,i_{j,l,r}} \neq 0$ for $1 \leq r \leq v$ and $a_{j,l,i} = 0$ for $i \in \{1, \ldots, n\} \setminus \{i_{j,l,1}, \ldots, i_{j,l,v}\}$. Then $\mu_{\alpha}(a_{j,l}) = \mu_{\alpha}(a_{j,l}) = i_{j,l,1} + \cdots + i_{j,l,\min(v,\alpha)}$. Let $i \in \{i_{j,l,1}, \ldots, i_{j,l,\min(v,\alpha)}\}$. Let the $i$th entries of $\tilde{a}_{j,l}, \ldots, \tilde{a}_{j,M} \in \mathbb{F}_q^n$ be given by $\alpha_1, \ldots, \alpha_M \in \mathbb{F}_q$, and let the $i$th entries of $c_{j,1}, \ldots, c_{j,M} \in \mathbb{F}_q^n$ be given by $\beta_1, \ldots, \beta_M \in \mathbb{F}_q$. By (4) we have

$$(\beta_1 \cdots \beta_M) = (\alpha_1 \cdots \alpha_M) \cdot A.$$

We have $j \leq s_l$ and hence $\tilde{a}_{j,l} = a_{j,l}$, and $\alpha_l \neq 0$ by the definition of $l$ and $i$. On the other hand, $\alpha_k = 0$ for $k > l$, as $\tilde{a}_{k,l} = 0$ for that case. Therefore we can write (6) as

$$(\beta_1 \cdots \beta_M) = (\alpha_1 \cdots \alpha_l) \cdot A_l.$$

In the following we show that there are at least $M - l + 1$ entries of $(\beta_1 \cdots \beta_M)$ which are non-zero. Assume to the contrary that there exist integers $1 \leq k_1 < \cdots < k_l \leq M$ such that $\beta_{k_1} = \cdots = \beta_{k_l} = 0$. Then we have

$$0 = (\beta_1 \cdots \beta_{k_l}) = (\alpha_1 \cdots \alpha_l) \cdot A(k_1, \ldots, k_l).$$

But as $\alpha_l \neq 0$ and $A(k_1, \ldots, k_l)$ is non-singular (as $A$ is NSC) it follows that $$(\beta_{k_1} \cdots \beta_{k_l}) \neq 0,$$

which yields a contradiction. Hence there are at least $M - l + 1$ entries of $(\beta_1 \cdots \beta_M)$ which are non-zero. As this holds for all $i \in \{i_{j,l,1}, \ldots, i_{j,l,\min(v,\alpha)}\}$ the result follows. \qed

**Lemma 3** Under the notation and assumptions above we have

$$\mu_{\alpha,n}(C) \geq (M - l + 1)\mu_{\alpha,n}(a_l).$$

**Proof.** We have $\mu_{\alpha,n}(C) = \sum_{k=1}^{M} \sum_{j=1}^{s_k} \mu_{\alpha}(c_{j,k})$ and $\mu_{\alpha,n}(a_l) = \mu_{\alpha}(a_{j_1,l}) + \cdots + \mu_{\alpha}(a_{j_u,l})$. Since $A$ is compatible with $(C_{1,l}^+, \ldots, C_{M,l}^+)$, we have $c_{j,k} = 0 \in \mathbb{F}_q^n$ for any $1 \leq k \leq M$ and $s_k < j \leq s$. Therefore, for each $1 \leq k \leq M$ we have

$$\sum_{j=1}^{s_k} \mu_{\alpha}(c_{j,k}) = \sum_{j=1}^{s} \mu_{\alpha}(c_{j,k}).$$

11
Hence
\[ \mu_{\alpha,n}(C) = \sum_{k=1}^{M} \sum_{j=1}^{s} \mu_{\alpha}(\mathcal{C}_{j,k}) = \sum_{j=1}^{s} \sum_{k=1}^{M} \mu_{\alpha}(\mathcal{C}_{j,k}) \geq \sum_{j \in \{j_1, \ldots, j_u\}} \sum_{k=1}^{M} \mu_{\alpha}(\mathcal{C}_{j,k}). \]

Lemma 2 now implies that
\[ \mu_{\alpha,n}(C) \geq (M - l + 1) \sum_{j \in \{j_1, \ldots, j_u\}} \mu_{\alpha}(\mathbf{a}_{j,l}) = (M - l + 1)\mu_{\alpha,n}(\mathbf{a}_l). \]

\[ \square \]

**Lemma 4** Let \( \mathcal{N} \) be the \( \mathbb{F}_q \)-linear subspace of \( \mathbb{F}_q^{n(s_1 + \cdots + s_M)} \) constructed above. Then
\[ \dim \mathcal{N} \geq \sum_{k=1}^{M} (ns_k - m_k), \]
and
\[ \delta_{\alpha,n}(\mathcal{N}) \geq \min_{1 \leq l \leq M} (M - l + 1)\delta_{\alpha,n}(\mathcal{C}_{l}^{-1}). \]

**Proof.** By the construction of \( \mathcal{N} \) we have \( \dim \mathcal{N} = \sum_{k=1}^{M} \dim \mathcal{C}_{k}^{-1} \). Since \( \dim \mathcal{C}_{k}^{-1} \geq ns_k - m_k \) the first result follows. The second result follows directly from Lemma 3. \( \square \)

The dual space of \( \mathcal{N}, \mathcal{N}^\perp \subseteq \mathbb{F}_q^{n(s_1 + \cdots + s_M)} \), satisfies \( \dim \mathcal{N}^\perp \leq m_1 + \cdots + m_M \). Let \( \mathcal{N}' \) be a generating matrix for \( \mathcal{N}^\perp \) and let \( m' \) be the number of rows of \( \mathcal{N} \). As \( \dim \mathcal{N}^\perp \leq m_1 + \cdots + m_M \), it follows that \( m' \leq m_1 + \cdots + m_M \). If \( m' < m_1 + \cdots + m_M \) we can add rows of zeroes to \( \mathcal{N}' \) to obtain a matrix \( \mathcal{N} \) which generates \( \mathcal{N} \) and has \( m = m_1 + \cdots + m_M \) rows.

We partition \( \mathcal{N} \) into submatrices \( \mathcal{N}_{1}, \mathcal{N}_{s_1 + \cdots + s_M} \), each of size \( m \times n \),
\[ \mathcal{N} = (\mathcal{N}_1 \mid \mathcal{N}_2 \mid \ldots \mid \mathcal{N}_{s_1 + \cdots + s_M}). \]

Then we define the generating matrices of the digital net by
\[ \mathbf{D}_j = \mathbf{N}_j^\top \text{ for } 1 \leq j \leq s_1 + \cdots + s_M. \tag{7} \]

**Remark 10** Instead of finding the generating matrices via the dual space, we can also write them down directly (note that the generating matrices are not unique, we only give one possible way of defining them; the point set is, up to a reordering of the points, always the same though):

For simplicity assume that \( A \) is an upper triangular NSC matrix over \( \mathbb{F}_q \). As \( A \) is a non-singular matrix, the diagonal elements \( A_{ij} \) are all non-zero and therefore have an inverse \( A_{ij}^{-1} \) in \( \mathbb{F}_q \). Let \( \sigma_0 = 0 \) and for \( 1 \leq k \leq M \) let \( \sigma_k = s_1 + \cdots + s_k \). Recall that \( \mathcal{C}''_{j,k} \in \mathbb{F}_q^{n \times m_k} \) and let \( \mathcal{A}^{n \times m} \) denote the \( n \times m \) zero matrix over \( \mathbb{F}_q \). Let \( m = m_1 + \cdots + m_M \). Then for \( 1 \leq k \leq M \) and \( \sigma_{k-1} < j \leq \sigma_k \) let
\[ \mathbf{D}_j = \left( \mathbf{0}^{n \times m_1} \ldots \mathbf{0}^{n \times m_{k-1}} \mathbf{V}_{k,k} \mathcal{C}'_{j-\sigma_{k-1},k} \ldots \mathbf{V}_{k,M} \mathcal{C}'_{j-\sigma_{k-1},M} \right) \in \mathbb{F}_q^{n \times m}, \]
where \( \mathbf{V}_{k,l} \in \mathbb{F}_q \) is given by: \( \mathbf{V}_{k,l} = 1 \) for \( 1 \leq k \leq M \) and for \( l = 1, \ldots, M - 1 \) we set
\[ \mathbf{V}_{k,k+l} = -A_{k,k+l}^{-1}(A_{k,k+l+1} \mathbf{V}_{k+1,k+l+1} + \cdots + A_{k,k} \mathbf{V}_{k+1,k+l}) \text{ for } 1 \leq k \leq M - l. \]

The matrices \( \mathbf{D}_1, \ldots, \mathbf{D}_{\sigma_M} \) are then the generating matrices of the digital net which has dual space \( \mathcal{N} \).
Theorem 6 (Propagation Rule IX) Assume we are given digital \((t_k, \alpha_k, \beta_k, n_k \times m_k, s_k)\)-nets, \(1 \leq k \leq M\), over \(\mathbb{F}_q\) and an \(M \times M\) NSC matrix \(A\).

Then the digital net constructed by the matrix-product propagation rule which is generated by \(D_1, \ldots, D_s \in \mathbb{F}_q^{n \times m}\) as in Equation (7), where \(s = s_1 + \cdots + s_M\), \(n = \max_{1 \leq k \leq M} n_k\), and \(m = m_1 + \cdots + m_M\), is a digital \((t, \alpha, \beta, n \times m, s)\)-net, where \(\beta = \min(1, \alpha m/n)\) and

\[
t = \beta n + 1 - \min_{1 \leq t \leq M} (M - l + 1)(\beta m_t - t + 1).
\]

Proof. In view of Remark 2 we only need to prove a bound on \(\beta n - t\) and choose \(\beta\) such that the requirements of Definition 2 are satisfied. Hence choosing \(\beta = \min(1, \alpha m/n)\) will be sufficient.

From Lemma 4 we obtain \(\delta_{\alpha,n}(N) \geq \min_{1 \leq t \leq M} (M - l + 1)\delta_{\alpha,n}(C_{i}^+\) and from Theorem 3 we obtain \(\delta_{\alpha,n}(C_{i}^+) \geq \beta_k n_k - t_k + 1 \geq 1 \leq k \leq M\). Therefore \(\delta_{\alpha,n}(N) \geq \min_{1 \leq t \leq M} (M - l + 1)(\beta_k n_k - t_k + 1)\). This implies that the linear independence condition in Definition 2 is satisfied if we choose \(t\) such that \(\beta n - t + 1 = \delta_{\alpha,n}(N)\), i.e., \(t = \beta n + 1 - \min_{1 \leq t \leq M} (M - l + 1)(\beta m_t - t + 1)\). Hence the result follows.

Theorem 6 can be generalized in the following ways: We assume now that we have given digital \((t_k, \alpha_k, \beta_k, n_k \times m_k, s_k)\)-nets, \(1 \leq k \leq M\), i.e., the \(\alpha\)-values of each digital net can be different. Let \(n' = n_1 + \cdots + n_M\), and let the first \(n\) rows of \(D_j\) be the first \(n\) rows of \(D_j\) and the remaining \(n' - n\) rows be \(0\). Then \(D_j' \in \mathbb{F}_q^{n' \times m}\) for \(1 \leq j \leq s_1 + \cdots + s_M\). Note that the point set obtained from using the generating matrices \(D_1, \ldots, D_{s_1 + \cdots + s_M}\) is the same as the one obtained from \(D_1', \ldots, D_{s_1 + \cdots + s_M}'\).

Corollary 1 Assume we are given digital \((t_k, \alpha_k, \beta_k, n_k \times m_k, s_k)\)-nets, \(1 \leq k \leq M\), over \(\mathbb{F}_q\) and an \(M \times M\) NSC matrix \(A\).

Then the digital net constructed by the matrix-product propagation rule, which is generated by \(D_1', \ldots, D_s' \in \mathbb{F}_q^{n' \times m}\), where \(s = s_1 + \cdots + s_M\), \(n' = n_1 + \cdots + n_M\), and \(m = m_1 + \cdots + m_M\), is a digital \((t', \alpha', \beta', n' \times m, s)\)-net, where \(\alpha' = \max_{1 \leq k \leq M} \alpha_k\), \(\beta' = \min_{1 \leq k \leq M} \beta_k\) and

\[
t' = \beta' n' + 1 - \min_{1 \leq l \leq M} (M - l + 1)(\beta m_t - t + 1).
\]

Proof. First we check that \(\beta' \leq \min(1, \alpha' m/n')\). We have \(\beta' = \min_{1 \leq k \leq M} \beta_k \leq 1\), as \(\beta_k \leq 1\). Hence it remains to show that \(\beta' n' \leq \alpha' m\). We have \(\beta_k n_k \leq \alpha_k m_k\) and hence

\[
\beta' n' = \beta n_1 + \cdots + \beta n_M \leq \beta_1 n_1 + \cdots + \beta M n_M \leq \alpha_1 m_1 + \cdots + \alpha M m_M \leq \alpha' m.
\]

As \(\alpha \geq \alpha_k\) we have \(\delta_{\alpha,n}(C_{i}^+) \geq \delta_{\alpha,n}(C_{i}^+) \geq \beta_k n_k - t_k \geq 1 \leq k \leq M\). Thus, using the same arguments as in the proof of Theorem 6, the result follows using Lemma 4.

Remark 11 For \(M = 2\) and

\[
A = \begin{pmatrix}
1 & 1 \\
0 & 1 \\
\end{pmatrix}
\]

the matrix-product construction yields the \((u, u+v)\)-construction. The generating matrices from Remark 10, augmented with enough rows of zeroes, are the same as in Section 3.2.

Remark 12 Although \(\beta\) and \(t\) are different in Theorem 6 and Corollary 1, the essential value is the strength of the digital net given by \(\beta n - t\), which is the same in both results.

Remark 13 Similar to Remark 6, one should use \(\alpha_1 = \cdots = \alpha_M\) in Corollary 1 in order to be able to obtain \(\beta n\) to be of order \(\alpha m\).
3.4 A double $m$ construction

In [10], Niederreiter and Pirsic introduced a propagation rule which used two digital nets, a digital $(t_1, m, s)$-net and a digital $(t_2, m, s)$-net, to construct a digital $(t, 2m, s)$-net. In the following we generalize this propagation rule to generalized digital nets.

Assume we are given two digital nets over the same finite field $\mathbb{F}_q$, a digital $(t_1, \alpha_1, \beta_1, n \times m, s)$-net with generating matrices $C_{1,1}, \ldots, C_{s,1} \in \mathbb{F}_q^{n \times m}$ and a digital $(t_2, \alpha_2, \beta_2, n \times m, s)$-net with generating matrices $C_{1,2}, \ldots, C_{s,2} \in \mathbb{F}_q^{n \times m}$. Then we consider the digital $(t, \alpha, \beta, 2n \times 2m, s)$-net with generating matrices $D_1, \ldots, D_s$ given by

$$D_j = \begin{pmatrix} C_{j,2} & C_{j,1} \\ -C_{j,2} & 0_{n \times m} \end{pmatrix}, \quad \text{for } 1 \leq j \leq s.$$  \hspace{1cm} (8)

In [10] the construction is described via the dual space. As in the previous sections, for $k = 1, 2$, we form the matrices

$$C_k = ((C_{1,k})^\top | \cdots | (C_{s,k})^\top).$$

The row space of $C_k$ is denoted by $C_k \subseteq \mathbb{F}_q^s$ and the dual space of $C_k$ is denoted by $C_k^\perp \subseteq \mathbb{F}_q^s$. For $k = 1, 2$, let $a_k = (a_{1,k} \ldots a_{s,k}) \in C_k^\perp$ and set

$$c = (a_{1,1}, a_{1,1} + a_{1,2}, a_{2,1}, a_{2,1} + a_{2,2}, \ldots, a_{s,1}, a_{s,1} + a_{s,2}) \in \mathbb{F}_q^{2ns}.$$  

Let the space of vectors $c$ obtained this way be denoted by $\mathcal{N}$, i.e.,

$$\mathcal{N} = \{ c \in \mathbb{F}_q^{2ns} : a_1 \in C_1^\perp, a_2 \in C_2^\perp \}.$$

We have

$$\dim(\mathcal{N}) = \dim(C_1^\perp) + \dim(C_2^\perp) \geq 2(sn - m),$$

and hence $\dim(\mathcal{N}^\perp) \leq 2sn - \dim(\mathcal{N}) \leq 2m$. Note that the space spanned by the rows of

$$E = (D_1^\top | \cdots | D_s^\top),$$

where $D_j$ is given by (8), is $\mathcal{N}^\perp$ and hence $\mathcal{N}$ is the dual space of the row space of $E$.

In order to bound the quality parameter for the digital net with generating matrices $D_1, \ldots, D_s$, we define

$$D(C_1^\perp, C_2^\perp) = \max_{1 \leq j \leq s} \max_{R_j} \max_{a_{j,1} + a_{j,2} = 0} (\mu_{a,n}(a_{j,1} + a_{j,2}) - \mu_{a,n}(a_{j,1} + a_{j,2})), $$

where $R_j$ is the set of all ordered pairs $(a_1, a_2)$, with $a_k = (a_{1,k} \ldots a_{s,k}) \in C_k^\perp \setminus \{0\}$, $a_{i,1} + a_{i,2} = 0$ for $i \neq j$ and $a_{j,1} + a_{j,2} \neq 0$. We define the maximum over $R_j$ to be zero if $R_j$ is empty.

**Theorem 7 (Propagation Rule X)** Let $C_{1,1}, \ldots, C_{s,1}$ be the generating matrices of a digital $(t_1, \alpha_1, \beta_1, n \times m, s)$-net and $C_{1,2}, \ldots, C_{s,2}$ be the generating matrices of a digital $(t_2, \alpha_2, \beta_2, n \times m, s)$-net over the same $\mathbb{F}_q$.

Then the digital net generated by $D_1, \ldots, D_s$ given by (8) is a digital $(t, \alpha, \beta, 2n \times 2m, s)$-net, where $\alpha = \max(\alpha_1, \alpha_2)$, $\beta = \min(\beta_1, \beta_2)$, and

$$t \leq \max(2\beta n - (1 + \beta_1)n + t_1 + D(C_1^\perp, C_2^\perp), 2\beta n - (1 + \beta_2)n + t_2),$$

if $C_1^\perp \cap C_2^\perp = \{0\}$, and

$$t \leq \max(2\beta n - (1 + \beta_1)n + t_1 + D(C_1^\perp, C_2^\perp), 2\beta n - (1 + \beta_2)n + t_2, 2\beta n + 1 - \delta_{\alpha,n}(C_1^\perp \cap C_2^\perp), 0)$$

if $C_1^\perp \cap C_2^\perp \neq \{0\}$. 

Proof. By the definition of $\alpha$ and $\beta$ it follows that $0 < \beta \leq 1$ and $2\beta n = \beta_1 n + \beta_2 n \leq \alpha_1 m + \alpha_2 m \leq 2\alpha m$. Hence the parameters $\alpha$ and $\beta$ are well defined according to Definition 2.

Using Theorem 3, it is sufficient to show that $2\beta n - t + 1$ is a lower bound on $\delta_{\alpha,2n}(N)$. Hence we only need to show a lower bound on $\mu_{\alpha,2n}(c)$ for all nonzero vectors $c$ in $N$.

In the proof we will use the property that $\delta_{\alpha,n}(C^\perp_k) \geq \delta_{\alpha,n}(C^\perp_1) \geq \beta_k n - t_k + 1$, as $\alpha \geq \alpha_k$ for $k = 1, 2$.

Let $c \in N$ be nonzero, then

$$\mu_{\alpha,2n}(c) = \sum_{j=1}^s \mu_\alpha(a_{j,1}, a_{j,1} + a_{j,2}).$$

We consider several cases. If $a_1 = 0$, then $a_2 \not= 0$ and therefore

$$\mu_{\alpha,2n}(c) \geq n + \sum_{j=1}^s \mu_\alpha(a_{j,2}) \geq n + \delta_{\alpha,n}(C^\perp_2) \geq n + \beta_2 n - t_2 + 1.$$ 

If $a_2 = 0$, then $a_1 \not= 0$ and analogously we obtain

$$\mu_{\alpha,2n}(c) \geq n + \sum_{j=1}^s \mu_\alpha(a_{j,1}) \geq n + \delta_{\alpha,n}(C^\perp_1) \geq n + \beta_1 n - t_1 + 1.$$ 

If $a_1, a_2 \not= 0$, but $a_1 + a_2 = 0$, then $a_1 \in C^\perp_1 \cap C^\perp_2$. If $C^\perp_1 \cap C^\perp_2 = \{0\}$, then this case is not possible. If $C^\perp_1 \cap C^\perp_2 \not= \{0\}$, then

$$\mu_{\alpha,2n}(c) = \mu_{\alpha,n}(a_1) \geq \delta_{\alpha,n}(C^\perp_1 \cap C^\perp_2).$$

The last case is where $a_1, a_2 \not= 0$ and $a_1 + a_2 \not= 0$. Then

$$\mu_{\alpha,2n}(c) \geq \sum_{j=1}^s \sum_{a_{j,1} + a_{j,2} \not= 0} (n + \mu_\alpha(a_{j,1} + a_{j,2})) + \sum_{j=1}^s \mu_\alpha(a_{j,1}).$$

If the first sum in the last expression has at least two terms, then $\mu_{\alpha,2n}(c) \geq 2n + 2$. Otherwise it has exactly one term, say for $j = j_0$, and then

$$\mu_{\alpha,2n}(c) \geq n + \mu_\alpha(a_{j_0,1} + a_{j_0,2}) + \sum_{j=1}^s \mu_\alpha(a_{j,1})$$

$$= n + \mu_{\alpha,n}(a_1) + \mu_\alpha(a_{j_0,1} + a_{j_0,2}) - \mu_\alpha(a_{j_0,1})$$

$$\geq n + \beta_1 n - t_1 + 1 - D(C^\perp_1, C^\perp_2).$$

Therefore we have

$$\delta_{\alpha,2n}(N) \geq \min((1 + \beta_1)n - t_1 + 1 - D(C^\perp_1, C^\perp_2), (1 + \beta_2)n - t_2 + 1)$$

if $C^\perp_1 \cap C^\perp_2 = \{0\}$, and

$$\delta_{\alpha,2n}(N) \geq \min((1 + \beta_1)n - t_1 + 1 - D(C^\perp_1, C^\perp_2), (1 + \beta_2)n - t_2 + 1, \delta_{\alpha,n}(C^\perp_1 \cap C^\perp_2))$$

if $C^\perp_1 \cap C^\perp_2 \not= \{0\}$. Thus the result follows.

\begin{remark}
Similar to Remark 6, one should use $\alpha_1 = \alpha_2$ in Theorem 7 in order to be able to obtain $\beta n$ to be of order $\alpha m$.
\end{remark}
3.5 A base change propagation rule

We state a result that is analogous to Theorem 9 in [11], which is sometimes also referred to as trace code for digital nets (cf. [13]).

**Theorem 8 (Propagation Rule XI)** Let $q$ be a prime power and $r$ be a positive integer. If $P$ is a digital $(t, \alpha, \beta, n \times m, s)$-net over $\mathbb{F}_{q'}$, then we can construct a digital $(t, \alpha, \beta, n \times rm, rs)$-net $Q$ over $\mathbb{F}_q$ from $P$.

**Proof.** The proof is of the same flavour as the proof of Theorem 9 in [11]. Let

$$D_{(j-1)r+k} := \begin{pmatrix} d_{i,(j-1)r+k} \\ \vdots \\ d_{n,(j-1)r+k} \end{pmatrix}, \quad 1 \leq j \leq s, \ 1 \leq k \leq r,$$

where $d_{i,(j-1)r+k} = \varphi(B_k c_{i,j})$ for $1 \leq i \leq n$, $1 \leq j \leq s$, $1 \leq k \leq r$. We claim that $Q$ is a digital $(t, \alpha, \beta, n \times rm, rs)$-net over $\mathbb{F}_q$.

Choose integers

$$1 \leq i_{(j-1)r+k, \nu_{(j-1)r+k}} < i_{(j-1)r+k, \nu_{(j-1)r+k-1}} < \cdots < i_{(j-1)r+k,1} \leq n$$

such that

$$\sum_{j=1}^{s} \sum_{k=1}^{r} \sum_{l=1}^{\nu_{(j-1)r+k}} \left( i_{(j-1)r+k,1} + \cdots + i_{(j-1)r+k,\min\{\nu_{(j-1)r+k}, \alpha\}} \right) \leq \beta n - t$$

and let $\delta^{(j,k)}_l \in \mathbb{F}_q$ such that

$$\sum_{j=1}^{s} \sum_{k=1}^{r} \sum_{l=1}^{\nu_{(j-1)r+k}} \delta^{(j,k)}_l d_{i_{(j-1)r+k,l,(j-1)r+k}} = 0 \in \mathbb{F}_q^m. \quad (9)$$

Due to the definition of the vectors $d_{i_{(j-1)r+k,l,(j-1)r+k}}$, (9) can be rewritten as

$$\sum_{j=1}^{s} \sum_{k=1}^{r} \sum_{l=1}^{\nu_{(j-1)r+k}} \delta^{(j,k)}_l \varphi(B_k c_{i_{(j-1)r+k,l,j}}) = 0 \in \mathbb{F}_q^m. \quad (10)$$

Now, let, for $1 \leq j \leq s$,

$$U_j := \bigcup_{k=1}^{r} \left\{ i_{(j-1)r+k,1}, \ldots, i_{(j-1)r+k,\nu_{(j-1)r+k}} \right\}.$$

Furthermore, for $1 \leq j \leq s$ and $1 \leq k \leq r$, put $\epsilon^{(j,k)}_l = 1$ if

$$l \in \left\{ i_{(j-1)r+k,1}, \ldots, i_{(j-1)r+k,\nu_{(j-1)r+k}} \right\}.$$
and \( e_{l}^{(j,k)} = 0 \) otherwise. Then (10) can be rewritten as
\[
\sum_{j=1}^{s} \sum_{k=1}^{r} \sum_{l \in U_{j}} e_{l}^{(j,k)} \delta_{l}^{(j,k)} \varphi \left( B_k c_{(i-1)r+k,l} \right) = 0 \in F_{q}^{r m}.
\]

Since \( \varphi \) is an \( F_{q} \)-linear isomorphism, we conclude that
\[
\sum_{j=1}^{s} \sum_{l \in U_{j}} \gamma_{l}^{(j)} c_{l,j} = 0 \in F_{q}^{m}
\]
with
\[
\gamma_{l}^{(j)} = \sum_{k=1}^{r} e_{l}^{(j,k)} \delta_{l}^{(j,k)} B_k \in F_{q}^{m}.
\]
Let us now consider
\[
\sum_{j=1}^{s} \sum_{l \in U_{j}} \gamma_{l}^{(j)} c_{l,j}.
\]
For \( 1 \leq j \leq s \), let \( \mu_{j} := |U_{j}| \) and denote the elements of \( U_{j} \), in increasing order, by \( g_{j,\mu_{j}} < g_{j,\mu_{j}-1} < \cdots < g_{j,1} \).

Note that we also have \( 1 \leq g_{j,\mu_{j}} \) and \( g_{j,1} \leq n \), and \( \sum_{j=1}^{s} \left( g_{j,1} + \cdots + g_{j,\min(\mu_{j},\alpha)} \right) \leq \beta n - t \), due to the order of \( g_{j,1}, \ldots, g_{j,\mu_{j}} \) and the conditions on the indices \( i_{(j-1)r+k,l} \) above. Thus, since the vectors \( c_{l,j} \) stem from the generating matrices of the digital \((t, \alpha, \beta, n \times m, s)\)-net \( P \), it follows that we must have \( \gamma_{l}^{(j)} = 0 \) for \( l \in U_{j} \), \( 1 \leq j \leq s \). hence, by (11), \( e_{l}^{(j,k)} \delta_{l}^{(j,k)} = 0 \) for \( l \in U_{j} \), \( 1 \leq j \leq s \), and \( 1 \leq k \leq r \). By the definition of the numbers \( e_{l}^{(j,k)} \), all coefficients \( \delta_{l}^{(j,k)} \) in (9) are zero. □

**Remark 15** As in [11, Theorem 9], the strength of the net obtained via this base change propagation rule stays unchanged, which is, \( \beta n - t \).

### 3.6 A dual space base change propagation rule

In this section we introduce another propagation rule, first established in [12], where we change the ground field from \( F_{q^{r}} \) to \( F_{q} \), for some prime power \( q \) and some positive integer \( r \). The difference to the previous propagation rule is that the \( F_{q} \)-linear transformation from \( F_{q^{r}} \) to \( F_{q}^{r} \) is now applied to the dual space instead of applying it to the generating matrices.

**Theorem 9 (Propagation Rule XII)** Given a digital \((t', \alpha, \beta, n \times m, s)\)-net over \( F_{q^{r}} \), we can construct a digital \((t, \alpha, \beta, rn \times rm, s)\)-net over \( F_{q} \), where
\[
t \leq rt' + (r - 1)(s\alpha - 1).
\]

**Proof.** Let \( \varphi : F_{q^{r}} \to F_{q}^{r} \) denote again an \( F_{q} \)-linear isomorphism. Let \( C_1, \ldots, C_s \in F_{q^{r}}^{n \times m} \) denote the generating matrices of the digital \((t', \alpha', \beta', n \times m, s)\)-net, and let \( C = (C_1^{T} | \cdots | C_s^{T}) \). The row space of \( C \) is denoted by \( \mathcal{C} \subseteq F_{q^{r}}^{m} \) and the dual space of \( \mathcal{C} \) by \( \mathcal{C}^{\perp} \subseteq F_{q^{r}}^{n} \).
a vector \( \mathbf{c} = (c_1, \ldots, c_s) \in C^\perp \), with \( c_j \in \mathbb{F}_{q^r} \), let \( \tilde{c}_j = \varphi(c_j) \in \mathbb{F}_{q^m} \) and \( \tilde{c} = (\tilde{c}_1, \ldots, \tilde{c}_s) \), where we extend the \( \mathbb{F}_{q^r} \)-linear isomorphism from \( \mathbb{F}_{q^r} \to \mathbb{F}_{q^m} \) componentwise, to an \( \mathbb{F}_{q^r} \)-linear isomorphism from \( \mathbb{F}_{q^r} \to \mathbb{F}_{q^m} \). Then we obtain a linear space \( \tilde{C}^\perp \subseteq \mathbb{F}_{q^m} \), by setting \( \tilde{C}^\perp = \{ \tilde{c} : \mathbf{c} \in C^\perp \} \).

Note that \( \dim_{\mathbb{F}_{q^r}}(\tilde{C}^\perp) = r \dim_{\mathbb{F}_{q^r}}(C^\perp) \), and \( \dim_{\mathbb{F}_{q^r}}(C^\perp) \geq sn - m \) by Proposition 2. Thus \( \dim_{\mathbb{F}_{q^r}}(\tilde{C}^\perp) \geq rsn - rm \), and the dual space of \( \tilde{C}^\perp \), denoted by \( \tilde{C} \), satisfies \( \dim_{\mathbb{F}_{q^r}}(\tilde{C}) \leq rm \).

Let \( \tilde{C} \in \mathbb{F}_{q^{rm \times rm}} \) be a matrix whose row space is \( \tilde{C} \), and let \( \tilde{C} = (D_1^\top | \cdots | D_s^\top) \), where \( D_j \in \mathbb{F}_{q^{rm \times rm}} \) for \( 1 \leq j \leq s \). The matrices \( D_1, \ldots, D_s \) now generate a digital net over \( \mathbb{F}_q \).

We now investigate the quality of this digital net. Let \( \tilde{c} \in \tilde{C}^\perp \) be a nonzero vector. We have \( \mu_\alpha,sn(\tilde{c}) = \mu_\alpha(\tilde{c}_1) + \cdots + \mu_\alpha(\tilde{c}_s) \). As \( \tilde{c} \) is nonzero, it follows that \( \mathbf{c} \) is nonzero. If \( \mu_\alpha(c_j) = 0 \), then \( c_j = 0 \) and hence \( \mathbf{c} \) is a zero vector.

Let \( \mu_\alpha(c_j) > 0 \), and \( \mathbf{c} = (c_1, \ldots, c_s) \). Let \( i_j, i_j > \cdots > i_{\nu_j} > 0 \) be the indices of the nonzero elements of \( \mathbf{c} \), i.e., \( c_{j_1, i_1} \neq 0 \) for \( 1 \leq v \leq \nu_j \) and \( c_{j_1, i_1} = 0 \) for \( i \notin \{i_1, \ldots, i_{\nu_j}\} \). Then \( \mathbf{c} = (\varphi(c_{j_1, 1}), \ldots, \varphi(c_{j_1, \nu_j})) \), and \( \varphi(c_{j_1, v}) \neq 0 \) for \( 1 \leq v \leq \nu_j \), and \( \varphi(c_{j_1, v}) = 0 \), for \( i \notin \{i_1, \ldots, i_{\nu_j}\} \). Then

\[
\mu_\alpha(c_j) \geq \sum_{u=1}^{\min(\alpha, \nu_j)} (r(i_{j,u} - 1) + 1) = r \sum_{u=1}^{\min(\alpha, \nu_j)} i_{j,u} - (r - 1) \min(\alpha, \nu_j) = r \mu_\alpha(c_j) - (r - 1) \alpha.
\]

The above inequality also holds if \( \mu_\alpha(c_j) = 0 \), hence

\[
\mu_\alpha,sn(\tilde{c}) \geq \sum_{j=1}^{s} \left[r \mu_\alpha(c_j) - (r - 1) \alpha\right] - (r - 1) \alpha = \sum_{j=1}^{s} \left[r \delta_\alpha,sn(c_j^\perp) - (r - 1) \alpha\right] \geq \beta n - t' + 1,
\]

As the last inequality holds for all nonzero \( \tilde{c} \in \tilde{C}^\perp \), it follows that \( \delta_\alpha,sn(\tilde{C}^\perp) \geq \beta n - t + 1 = \delta_\alpha,sn(C^\perp) \). Using \( \delta_\alpha,sn(C^\perp) \geq \beta n - t' + 1 \), the result follows.

### 3.7 A base change propagation rule for projective spaces

In this section we generalize a propagation rule for digital nets which appears in MinT [13] under the name “base reduction for projective spaces”. Let \( r \geq 1 \). Let \( C_1, \ldots, C_s \in \mathbb{F}_{q^{rm \times m}} \) be the generating matrices of a digital \((t, \alpha, \beta, n \times m, s)\)-net. Note that the linear independence condition in Definition 2 stays unchanged if we multiply a row of \( C_j \) with some nonzero element in \( \mathbb{F}_{q^r} \). Doing so, we can obtain generating matrices \( C'_1, \ldots, C'_s \in \mathbb{F}_{q^{rm \times m}} \), which also generate a digital \((t, \alpha, \beta, n \times m, s)\)-net, and for which the first column of each \( C'_j \) only consists of zeroes and ones.

Let \( \varphi \) be an \( \mathbb{F}_{q^r} \)-linear isomorphism from \( \mathbb{F}_{q^r} \) to \( \mathbb{F}_{q^m}^r \) such that \( \varphi(1) = (0, \ldots, 0, 1) \in \mathbb{F}_{q^m}^r \). For a vector \( \mathbf{c} \in \mathbb{F}_{q^r}^m \) with \( \mathbf{c} = (c_1, \ldots, c_m) \) we define \( \varphi(\mathbf{c}) = (\varphi(c_1), \ldots, \varphi(c_m)) \in \mathbb{F}_{q^m}^r \), and for a matrix \( C \in \mathbb{F}^{n \times rm}_{q^r} \) with \( C = (c_1^\top, \ldots, c_n^\top)^\top \), we define \( \varphi(C) = (\varphi(c_1)^\top, \ldots, \varphi(c_n)^\top)^\top \in \mathbb{F}^{n \times rm}_{q^r} \).

For \( 1 \leq j \leq s \) let now \( D'_j = \varphi(C'_j) \in \mathbb{F}^{n \times rm}_{q^r} \). Note that the first \( r - 1 \) columns of \( D'_j \) are zero for each \( j = 1, \ldots, s \), as the first column of \( C'_j \) consists only of zeroes and ones. Let \( D'_j \in \mathbb{F}^{n \times (rm - (r - 1))}_{q^r} \) be the matrix obtained by discarding the first \( r - 1 \) rows of \( D'_j \). Then, because we only discarded zeroes, the strength of the digital net with generating matrices \( D_j \) is the same as the strength of the digital net with generating matrices \( D'_j \). From the proof of Theorem 8 we obtain that the strength of the digital net generated by \( D'_1, \ldots, D'_s \)
Proof. Let \( \emptyset \) the largest integer such that there are matrices \( C'_1, \ldots, C'_s \), which in turn is the same as the strength of the digital net with generating matrices \( C_1, \ldots, C_s \). Thus we obtain the following result.

**Theorem 10 (Propagation Rule XIII)** Let \( r \geq 1 \). Given a digital \( (t, \alpha, \beta, n \times m, s) \)-net over \( \mathbb{F}_{q}^r \), using the construction outlined in this section, we can obtain a digital \( (t, \alpha, \beta, n \times (rm - r + 1), s) \)-net over \( \mathbb{F}_{q} \).

### 3.8 A higher order to higher order construction

In [4] an explicit construction of digital \( (t, \alpha, \beta, n \times m, s) \)-nets was introduced which is based on classical \( (t, m, s) \)-nets. This can also be viewed as a propagation rule, which we generalize in the following.

Let \( d \geq 1 \) and let \( C_1, \ldots, C_{sd} \in \mathbb{F}_q^{n \times m} \) be the generating matrices of a digital \( (t, \alpha, \beta, n \times m, sd) \)-net over \( \mathbb{F}_q \). Let \( C_j = (c_{j,1}^\top, \ldots, c_{j,n}^\top) \) for \( j = 1, \ldots, sd \), i.e., \( c_{j,l} \) is the \( l \)th row of \( C_j \). Now let the matrix \( D_j \) be made of the first rows of the matrices \( C_{(j-1)d+1}, \ldots, C_{jd} \), and so on. The matrix \( D_j \) is then a \( dn \times m \) matrix, i.e., \( D_j = ((d_{j,1})^\top, \ldots, (d_{j,dn})^\top)^\top \), where \( d_{j,l} = c_{u,v} \) with \( l = (v - j)d + u \), \( 1 \leq v \leq n \), and \( (j - 1)d < u \leq jd \) for \( l = 1, \ldots, dn \) and \( j = 1, \ldots, s \). The following result is a generalization of [4, Theorem 4.11] (see also [3, Theorem 4.1]).

**Theorem 11 (Propagation Rule XIV)** Let \( d \geq 1 \) be a natural number and let \( C_1, \ldots, C_{sd} \) be the generating matrices of a digital \( (t', \alpha', n \times m, sd) \)-net over the finite field \( \mathbb{F}_q \). Let \( D_1, \ldots, D_s \) be defined as above. Then for any \( \alpha \geq 1 \) the matrices \( D_1, \ldots, D_s \) are generating matrices of a digital \( (t, \alpha, \beta' \min(1, \alpha/(\alpha'd)), dn \times m, s) \)-net over \( \mathbb{F}_q \) with

\[
\begin{align*}
    t &\leq \left\lfloor \min(d, \alpha/\alpha') t' + \frac{s(d - 1) \min(\alpha, \alpha'd)}{2} \right\rfloor
\end{align*}
\]

**Proof.** Let \( D_j = ((d_{j,1})^\top, \ldots, (d_{j,dn})^\top)^\top \) for \( j = 1, \ldots, s \) and further let the integers \( i_{1,1}, \ldots, i_{1,v_1}, \ldots, i_{s,1}, \ldots, i_{s,v_s} \) be such that \( 1 \leq i_{j,v_j} < \cdots < i_{j,1} \leq dn \) and

\[
    i_{1,1} + \cdots + i_{1,\min(v_1,\alpha)} + \cdots + i_{s,1} + \cdots + i_{s,\min(v_s,\alpha)} \leq \beta' \min(1, \alpha/(\alpha'd))dn - t.
\]

We need to show that the vectors

\[
d_{1,i_{1,1}}, \ldots, d_{1,i_{1,v_1}}, \ldots, d_{s,i_{s,1}}, \ldots, d_{s,i_{s,v_s}}
\]

are linearly independent over \( \mathbb{F}_q \).

For \( j = 1, \ldots, s \) let \( U_j = \{d_{j,i_{j,v_j}}, \ldots, d_{j,i_{j,1}}\} \). The vectors in the set \( U_j \) stem from the matrices \( C_{(j-1)d+1}, \ldots, C_{jd} \). For \( j = 1, \ldots, s \) and \( f_j = (j - 1)d + 1, \ldots, jd \), let \( w_{f_j} \geq 0 \) be the largest integer such that there are \( e_{f_j,1} > \cdots > e_{f_j,w_{f_j}} > 0 \) with \( \{e_{f_j,u} - j\}d + f_j : u = 1, \ldots, w_{f_j} \subseteq \{i_{j,v_j}, \ldots, i_{j,1}\} \), where for \( w_{f_j} = 0 \) we set \( \{(e_{f_j,u} - j)d + f_j : u = 1, \ldots, w_{f_j}\} = \emptyset \).

Let \( \alpha'd \leq \alpha \). For a given \( 1 \leq j \leq s \) we have

\[
    \sum_{f_j=(j-1)d+1}^{jd} \left( \sum_{r=1}^{\min(\alpha',w_{f_j})} d(e_{f_j,r} - 1) + \min(\alpha',w_{f_j})(f_j - (j - 1)d) \right) \leq i_{j,1} + \cdots + i_{j,\min(v_j,\alpha'd)}.
\]

19
Further we have
\[
\sum_{f_j=(j-1)d+1}^{jd} \left( \min(\alpha', w_{f_j}) \sum_{r=1}^{\min(\alpha', w_{f_j})} d(e_{f_j,r} - 1) + \min(\alpha', w_{f_j})(f_j - (j-1)d) \right)
\]
\[
= \sum_{f_j=(j-1)d+1}^{jd} \left( \min(\alpha', w_{f_j}) \sum_{r=1}^{\min(\alpha', w_{f_j})} de_{f_j,r} + \min(\alpha', w_{f_j})(f_j - jd) \right)
\]
\[
\geq \sum_{f_j=(j-1)d+1}^{jd} \sum_{r=1}^{\min(\alpha', w_{f_j})} de_{f_j,r} - \alpha' \frac{d(d - 1)}{2}.
\]
Thus it follows that
\[
d \sum_{j=1}^{s} \sum_{f_j=(j-1)d+1}^{jd} \sum_{r=1}^{\min(\alpha', w_{f_j})} e_{f_j,r} \leq \sum_{j=1}^{s} (i_{j,1} + \cdots + i_{j,\min(\nu_j, \alpha)}) + s \alpha' \frac{d(d - 1)}{2}
\]
\[
\leq \beta' \min(1, \alpha/\alpha')dn - t + s \alpha' \frac{d(d - 1)}{2}
\]
and therefore
\[
\sum_{j=1}^{s} \sum_{f_j=(j-1)d+1}^{jd} \sum_{r=1}^{\min(\alpha', w_{f_j})} e_{f_j,r} \leq \beta' n - \frac{t}{d} + s \alpha' \frac{d(d - 1)}{2} \leq \beta' n - t'.
\]
Thus it follows from the digital \((t', \alpha', \beta', n \times m, sd)\)-net property of the digital net generated by \(C_1, \ldots, C_{sd}\) that the vectors \(d_{1,i_1,1}, \ldots, d_{1,i_1,\nu_1}, \ldots, d_{s,i_s,1}, \ldots, d_{s,i_s,\nu_s}\) are linearly independent.

Let now \(\alpha' > \alpha\). For a given \(1 \leq j \leq s\) we have
\[
\sum_{f_j=(j-1)d+1}^{jd} \left( \min(\alpha', w_{f_j}) \sum_{r=1}^{\min(\alpha', w_{f_j})} d(e_{f_j,r} - 1) + \min(\alpha', w_{f_j})(f_j - (j-1)d) \right)
\]
\[
\leq i_{j,1} + \cdots + i_{j,\min(\nu_j, \alpha)} + (\alpha' d - \alpha)i_{j,\min(\nu_j, \alpha)}.
\]
Hence we can use inequality (12) again. Note that
\[
i_{1,\min(\nu_1, \alpha)} + \cdots + i_{s,\min(\nu_s, \alpha)} \leq \beta' \min(1/\alpha, 1/\alpha')dn - t/\alpha
\]
and hence we have
\[
\sum_{j=1}^{s} (i_{j,1} + \cdots + i_{j,\min(\nu_j, \alpha)} + (\alpha' d - \alpha)i_{j,\min(\nu_j, \alpha)})
\]
\[
\leq \beta' \min(1, \alpha/\alpha')dn - t + (\alpha' d - \alpha)(\beta' \min(1/\alpha, 1/\alpha')dn - t/\alpha)
\]
\[
= \beta' \min(\alpha' d/\alpha, 1)dn - t\alpha' d/\alpha.
\]
Thus it follows that
\[
d \sum_{j=1}^{s} \sum_{f_j=(j-1)d+1}^{jd} \sum_{r=1}^{\min(\alpha', w_{f_j})} e_{f_j,r}
\]

20
\[ \leq \sum_{j=1}^{s} (i_{j,1} + \cdots + i_{j,\min(t,\alpha)}) + (\alpha' d - \alpha) i_{j,\min(t,\alpha)} + s\alpha' d(d-1) \]

\[ \leq \beta' \min(\alpha' d/\alpha, 1)dn - t\alpha' d/\alpha + s\alpha' d(d-1) \]

and therefore

\[ \sum_{j=1}^{s} \sum_{j=1}^{d} \sum_{r=1}^{\min(\alpha', w_{f_j})} e_{f_j, r} \leq \beta'n - t\alpha' + s\alpha' d(d-1) \]

Thus it follows from the digital \((t', \alpha', \beta', n \times m, s\alpha')\)-net property of the digital net generated by \(C_1, \ldots, C_{sd}\) that the vectors \(d_{1,i_1,1}, \ldots, d_{1,i_1,\nu_1}, \ldots, d_{n,i_n,1}, \ldots, d_{n,i_n,\upsilon_n}\) are linearly independent and hence the result follows. \(\Box\)

4 Numerical Results

The results in Section 3 allow the construction of a digital \((t, \alpha, \beta, n \times m, s)\)-net from other existing (generalized) digital nets. In the following we present some examples where we can improve on the construction from [4].

In Tables 1, 2, and 3, we present, for selected values of \(m, q, \) and \(s\), the results obtained when we use different propagation rules for the cases \(\alpha = 2\) and \(\beta = 1\). Table 1 covers the case where \(q = 2\) for \(s = 15\) and \(s = 25\), Tables 2 and 3 the cases \(q = 3\) and \(q = 5\), respectively, for the same choices of \(s\). In both tables we consider \(m\) between 15 and 30. Since \(\alpha\) and \(\beta\) are fixed, and different propagation rules might yield different ratios of \(n\) and \(m\), it is most useful to compare the strengths of the nets obtained. As outlined in Remark 2, the strength of a digital net refers to the value of \(\sigma = \sigma(\beta, n, t) = \beta n - t\). Note that, in some of our new propagation rules, one can make many different choices of smaller nets that might (or might not) yield a bigger net with the same parameters. For example, a \((t, 2, 60 \times 30, 25)\)-net could be constructed using Propagation Rule VII from a \((t, 2, 40 \times 20, 20)\)-net together with a \((t, 2, 20 \times 10, 5)\)-net or from a \((t, 2, 30 \times 15, 10)\)-net together with a \((t, 2, 30 \times 15, 15)\)-net or several other combinations. In our tables, we only give the best values of the strength \(\sigma\) we can obtain by going through all possible choices of the smaller nets involved.

In Tables 1, 2, and 3, we compare the following quantities.

- \(\sigma_{\text{dir}}\): The strength of a digital \((t, \alpha, 1, \alpha m \times m, s)\)-net over \(\mathbb{F}_q\) using the generating matrices of an existing classical digital \((t', m, \alpha s)\)-net over \(\mathbb{F}_q\), where we then obtain (cf. [4])

\[ t \leq \min \left\{ \alpha m, \alpha t' + \alpha (\alpha - 1) \right\}. \]

(See also Theorem 11, which is a generalization of the result in [4]. Further, see [5] for constructions of polynomial lattice rules.) In the following we refer to this construction method as the direct construction method.

- \(\sigma_{\text{VIII}}\): The strength of a digital net constructed from a digital \((t_1, \alpha, \alpha m_1 \times m_1, s_1)\)-net \(P_1\) and a digital \((t_2, \alpha, \alpha m_2 \times m_2, s_2)\)-net \(P_2\) over \(\mathbb{F}_q\) using Propagation Rule VII (see Section 3.1), where \(P_1\) and \(P_2\) are obtained by the direct construction method from classical nets. Here, \(n = \alpha m\).
Table 1: $\sigma$-values depending on $m$ ($15 \leq m \leq 30$) for $\alpha = 2$, $\beta = 1$, $q = 2$, and $s = 15$ (left), $s = 25$ (right).

<table>
<thead>
<tr>
<th>$m$</th>
<th>$\sigma_{\text{dir}}$</th>
<th>$\sigma_{\text{VIII}}$</th>
<th>$\sigma_{\text{VIII}}$</th>
<th>$\sigma_{\text{XI}}$</th>
<th>$m$</th>
<th>$\sigma_{\text{dir}}$</th>
<th>$\sigma_{\text{VIII}}$</th>
<th>$\sigma_{\text{VIII}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>15</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
<td>16</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td></td>
<td>17</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>18</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>18</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>19</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td></td>
<td>19</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>20</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td></td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>21</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>7</td>
<td>21</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>22</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td></td>
<td>22</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>23</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td></td>
<td>23</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>24</td>
<td>1</td>
<td>4</td>
<td>6</td>
<td>9</td>
<td>24</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>25</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td></td>
<td>25</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>26</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td></td>
<td>26</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>27</td>
<td>5</td>
<td>6</td>
<td>9</td>
<td>11</td>
<td>27</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>28</td>
<td>7</td>
<td>7</td>
<td>10</td>
<td></td>
<td>28</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>29</td>
<td>9</td>
<td>9</td>
<td>10</td>
<td></td>
<td>29</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>30</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>13</td>
<td>30</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

- $\sigma_{\text{VIII}}$: The strength of a digital net constructed from a digital $(t_1, \alpha, \alpha m_1 \times m_1, s_1)$-net $P_1$ and a digital $(t_2, \alpha, \alpha m_2 \times m_2, s_2)$-net $P_2$ ($s_1 \leq s_2$) over $\mathbb{F}_q$ using Propagation Rule VIII (see Section 3.2), where $P_1$ and $P_2$ are obtained by the direct construction method from classical nets. Here, $n = \alpha m$.

- $\sigma_{\text{IX}}$: The strength of a digital net constructed from a digital $(t_1, \alpha, \alpha m_1 \times m_1, s_1)$-net $P_1$, a digital $(t_2, \alpha, \alpha m_2 \times m_2, s_2)$-net $P_2$, and a digital $(t_3, \alpha, \alpha m_3 \times m_3, s_3)$-net $P_3$ ($s_1 \leq s_2 \leq s_3$) over $\mathbb{F}_q$ using Propagation Rule IX (see Section 3.3), where $P_1$, $P_2$, and $P_3$ are obtained by the direct construction method from classical nets. Note that this propagation rule is only applicable for $q = 3, 5$. Again, $n = \alpha m$.

- $\sigma_{\text{XI}}$: The strength of a digital net obtained by using Propagation Rule XI with $r = 3$. Since the $t$-values of classical digital nets over $\mathbb{F}_{5^3} = \mathbb{F}_{125}$ are hardly available, we restrict ourselves to the bases 2 and 3 here. Furthermore, since 3 is not a divisor of 25, $\sigma_{\text{XI}}$ does not occur in Table for dimension $s = 25$. For $\sigma_{\text{XI}}$ we have $n = \alpha(m/3)$ (provided that $m$ is a multiple of 3).

We emphasize that our examples are just illustrations and by no means can systematically cover all cases one might theoretically consider; to be more precise, we have the following restrictions in Tables 1–3.

- Not all of the fourteen propagation rules occurring in Section 3 are represented in the tables. Furthermore, we only show particular choices of the parameters involved. We restrict ourselves to some cases where considerable improvement can be observed.

- We do not consider combinations of different propagation rules. Each of the values in Tables 1–3 is obtained by applying only one propagation rule (plus the direct construction method) at once.
Table 2: $\sigma$-values depending on $m$ ($15 \leq m \leq 30$) for $\alpha = 2$, $\beta = 1$, $q = 3$, and $s = 15$ (left), $s = 25$ (right).

<table>
<thead>
<tr>
<th>$m$</th>
<th>$\sigma_{\text{dir}}$</th>
<th>$\sigma_{\text{VII}}$</th>
<th>$\sigma_{\text{VIII}}$</th>
<th>$\sigma_{\text{IX}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>16</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>17</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>18</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>19</td>
<td>3</td>
<td>4</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>20</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>21</td>
<td>5</td>
<td>5</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>22</td>
<td>5</td>
<td>6</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>23</td>
<td>7</td>
<td>7</td>
<td>9</td>
<td>11</td>
</tr>
<tr>
<td>24</td>
<td>7</td>
<td>8</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>25</td>
<td>9</td>
<td>9</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>9</td>
<td>13</td>
<td>12</td>
</tr>
<tr>
<td>27</td>
<td>11</td>
<td>11</td>
<td>13</td>
<td>12</td>
</tr>
<tr>
<td>28</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>30</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
</tr>
</tbody>
</table>

Table 3: $\sigma$-values depending on $m$ ($15 \leq m \leq 30$) for $\alpha = 2$, $\beta = 1$, $q = 5$, and $s = 15$ (left), $s = 25$ (right).

<table>
<thead>
<tr>
<th>$m$</th>
<th>$\sigma_{\text{dir}}$</th>
<th>$\sigma_{\text{VII}}$</th>
<th>$\sigma_{\text{VIII}}$</th>
<th>$\sigma_{\text{IX}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>0</td>
<td>3</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>16</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>17</td>
<td>1</td>
<td>4</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>18</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>19</td>
<td>3</td>
<td>5</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>20</td>
<td>5</td>
<td>6</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>21</td>
<td>7</td>
<td>7</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>22</td>
<td>7</td>
<td>8</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>23</td>
<td>9</td>
<td>9</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>24</td>
<td>11</td>
<td>11</td>
<td>14</td>
<td>15</td>
</tr>
<tr>
<td>25</td>
<td>13</td>
<td>13</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>26</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>27</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>28</td>
<td>19</td>
<td>19</td>
<td>19</td>
<td>19</td>
</tr>
<tr>
<td>29</td>
<td>21</td>
<td>21</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>30</td>
<td>23</td>
<td>23</td>
<td>23</td>
<td>23</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$m$</th>
<th>$\sigma_{\text{dir}}$</th>
<th>$\sigma_{\text{VII}}$</th>
<th>$\sigma_{\text{VIII}}$</th>
<th>$\sigma_{\text{IX}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>0</td>
<td>3</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>16</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>17</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>18</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>19</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>20</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>21</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>22</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>23</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>24</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>25</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>26</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>27</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>8</td>
</tr>
<tr>
<td>28</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>29</td>
<td>5</td>
<td>5</td>
<td>6</td>
<td>9</td>
</tr>
<tr>
<td>30</td>
<td>5</td>
<td>5</td>
<td>6</td>
<td>9</td>
</tr>
</tbody>
</table>
• Not all propagation rules are applicable for all sets of parameters. This is indicated by void cells in the tables in cases where a certain propagation rule was not applicable.

A more systematic approach, taking into account more combinations of parameters and different propagation rules, would be very interesting and would certainly lead to further improvements. However, due to the vast number of choices, we leave this systematic approach open for future research.

Acknowledgements

The authors would like to thank W. Ch. Schmid and R. Schürer for valuable comments. The authors gratefully acknowledge the support of the ARC under its Centres of Excellence Program.

References


[8] Niederreiter, H.: Constructions of \((t, m, s)\)-nets and \((t, s)\)-sequences. Finite Fields Appl. 11, 578–600, 2005.


Authors’ address:
School of Mathematics and Statistics
University of New South Wales
Sydney, NSW, 2052
Australia

E-mail: \{josef.dick;p.kritzer\}@unsw.edu.au