MATHEMATICS OF COMPUTATION
Volume 79, Number 270, April 2010, Pages 993–1017
S 0025-5718(09)02315-1
Article electronically published on November 17, 2009

DUALITY THEORY AND PROPAGATION RULES FOR GENERALIZED DIGITAL NETS

JOSEF DICK AND PETER KRITZER

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 the 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.

1. INTRODUCTION

Often it is necessary to approximate a high dimensional integral $\int_{[0,1]^s} f(\mathbf{x})\,\mathrm{d}\mathbf{x}$ 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 $\frac{1}{N}\sum_{h=0}^{N-1} f(\mathbf{x}_h)$. As quadrature points one can use a so-called digital (t,m,s)-net. Classical digital (t,m,s)-nets were introduced by Niederreiter [7] (see also [8]). 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 [8].

In [5], 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 [7] and [5] 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 $C_1,\dots,C_s$ 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 $0\le h<q^m$ let $h=h_0+h_1q+\cdots+h_{m-1}q^{m-1}$ be the base q representation of h. Consider an arbitrary but fixed bijection $\eta:\{0,1,\dots,q-1\}\to\mathbb{F}_q$, where $\eta(0)$ is the zero element in $\mathbb{F}_q$. Identify

Received by the editor August 29, 2008 and, in revised form, April 9. 2009.
2000 *Mathematics Subject Classification.* Primary 11K38, 11K45, 65C05, 94B05.
Key words and phrases. Quasi-Monte Carlo, numerical integration, digital nets, duality theory, propagation rules.
The support of the Australian Research Council under its Centre of Excellence program is gratefully acknowledged.

h with the vector $\mathbf{h} := (\eta(h_0), \dots, \eta(h_{m-1})) \in \mathbb{F}_q^m$. For $1 \le j \le s$, we multiply the matrix C_j by $\mathbf{h}$, i.e.,

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

and set

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

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

As 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 $C_1, \dots, C_s$. These properties are, in the currently most general form of digital nets as introduced in [5], described by additional parameters t, α, β, which is why those nets are referred to as $(t, \alpha, \beta, n \times m, s)$-nets. The exact role of the parameters t, α and β is stated in the following definition.

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

$$i_{1,1} + \cdots + i_{1,\min\{\nu_1,\alpha\}} + \cdots + i_{s,1} + \cdots + i_{s,\min\{\nu_s,\alpha\}} \le \beta n - t, \tag{1}$$

the vectors

$$\vec{c}_{1,i_{1,\nu_1}}, \dots, \vec{c}_{1,i_{1,1}}, \dots, \vec{c}_{s,i_{s,\nu_s}}, \dots, \vec{c}_{s,i_{s,1}} \tag{2}$$

are linearly independent over $\mathbb{F}_q$.

If t is the smallest non-negative integer such that the digital net generated by $C_1, \dots, C_s$ 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 $\nu_1 + \cdots + \nu_s \le m$ holds whenever (1) is satisfied. (Note that $\nu_j \le i_{j,1}$.)

Remark 2. W.l.o.g. β in Definition 2 may be chosen such that βn is an integer, although in the formulae below it is often more convenient to define β in a way which does not guarantee that βn is an integer. This does not affect the quality of the net, as the left hand side of (1) is always an integer (therefore one could always replace βn with $\lfloor \beta n \rfloor$).

Remark 3. Without loss of generality we added the condition that $\beta \le 1$ 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 β 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 [5, Remark 5.3] we can therefore assume without loss of generality that $\beta \le 1$.

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 β and t then disappears; see [5] 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 4. As already indicated in Remark 3, 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 the 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. [15]).

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 $\{\mathbf{x}_0, \ldots, \mathbf{x}_{q^m-1}\}$ 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*

$$\left| \int_{[0,1]^s} f(\mathbf{x})\, \mathrm{d}\mathbf{x} - \frac{1}{q^m} \sum_{h=0}^{q^m-1} f(\mathbf{x}_h) \right| = \mathcal{O}\left(q^{-(\beta n - t)} (\beta n - t)^{\alpha s} \right).$$

For $\alpha = 1$ this is a classical result, see for example [8], and for $\alpha > 1$, see [5]. 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 [2, 9, 11, 13] and also the survey article [10], 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 [15], 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 [15]), 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 [5]. 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 [5]; for a proof, see [4, Theorem 3.3]. For completeness we repeat them in the following theorem, and we 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 $C_1, \ldots, C_s \in \mathbb{F}_q^{n \times m}$ (we assume that βn is an integer). Then we have the following:*

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

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

(iii) *Let $1 \le n' \le n$. Then the matrices $C_1^{(n')}, \dots, C_s^{(n')}$, 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 $t' = \max(\lfloor t - \beta(n - n') \rfloor, 0)$.*

(iv) *Let $n' \ge n$. Then the generating matrices $C_1^{(n')}, \dots, C_s^{(n')}$, where the first n rows of $C_j^{(n')}$ are the same as those of C_j and the remaining $n' - n$ rows are $\mathbf{0} = (0, \dots, 0) \in \mathbb{F}_q^m$, generate a digital $(t, \alpha, \beta', n' \times m, s)$-net, where $\beta' = \beta n/n'$.*

(v) *Let $1 \le s' \le s$ and $u \subseteq \{1, \dots, s\}$ 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 $1 \le j \le s$, let $C_j' \in \mathbb{F}_q^{n \times (m+v)}$ be the matrix obtained by augmenting C_j with v columns of $\mathbf{0}^\top = (0, \dots, 0)^\top \in \mathbb{F}_q^n$. Then $C_1', \dots, C_s'$ 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 [12] 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. [10]), the $(u, u+v)$-construction [2], the matrix-product construction [11], three different base change propagation rules [13, 14, 15] and the construction of higher order nets [5].

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 [12] to digital $(t, \alpha, \beta, n \times m, s)$-nets. Given generating matrices $C_1, \dots, C_s$ of a generalized digital net, let

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

The row space of C, denoted by $\mathscr{C}$, is a linear subspace of $\mathbb{F}_q^{sn}$. We define the dual space $\mathcal{N}$ of $\mathscr{C}$ 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 $\mathbf{a} = (a_1, \dots, a_n)$, where the only non-zero elements are $a_{i_1}, a_{i_2}, \dots, a_{i_v}$, with $n \ge i_1 > i_2 > \cdots > i_v \ge 1$, let $\mu_\alpha(\mathbf{a}) = i_1 + \cdots + i_{\min(\alpha, v)}$. For vectors $\mathbf{A} = (\mathbf{a}^{(1)}, \dots, \mathbf{a}^{(s)}) \in \mathbb{F}_q^{sn}$, with $\mathbf{a}^{(i)} \in \mathbb{F}_q^n$ for $1 \le i \le s$, we define

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

Remark 5. For $\alpha = 1$ we obtain the definition of the quantity V_m in [12].

The following definition is analogous to [12, Definition 2].

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 [12, 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 [12, Proposition 1]. We put $(x)_+ = \max(x, 0)$.

Proposition 1. *Let $\mathcal{N}$ be a non-zero linear subspace of $\mathbb{F}_q^{sn}$ with $\dim(\mathcal{N}) - 1 = rn + u$, where $0 \leq u < n$ and $0 \leq r < s$. Then we have*

$$\begin{aligned}\delta_{\alpha,n}(\mathcal{N}) \quad \leq \quad & (s-r-1)[n + (n-1) + (n-2)_+ + \cdots + (n-\alpha+1)_+] \\ & +(n-u) + (n-u-1) + (n-u-2)_+ + \cdots + (n-u-\alpha+1)_+.\end{aligned}$$

Proof. Let $h = \dim(\mathcal{N}) \geq 0$. Let $\pi : \mathcal{N} \to \mathbb{F}_q^{h+1}$ be the linear transformation which maps $\mathbf{A} \in \mathcal{N}$ to the $(h+1)$-tuple of the last $h+1$ coordinates of $\mathbf{A}$. If π is surjective, then there exists a non-zero $\mathbf{A}_1 \in \mathcal{N}$ with

$$\pi(\mathbf{A}_1) = (1, 0, \ldots, 0) \in \mathbb{F}_q^{h+1};$$

i.e., the last h coordinates of $\mathbf{A}_1$ are 0. Then

$$\begin{aligned}\mu_{\alpha,n}(\mathbf{A}_1) \quad \leq \quad & (s-r-1)[n + (n-1) + (n-2)_+ + \cdots + (n-\alpha+1)_+] \\ & +(n-u) + (n-u-1) + (n-u-2)_+ + \cdots + (n-u-\alpha+1)_+.\end{aligned}$$

If π is not surjective, then for any $\mathbf{A}_2$ in the kernel of π we have

$$\begin{aligned}\mu_{\alpha,n}(\mathbf{A}_2) \quad < \quad & (s-r-1)[n + (n-1) + (n-2)_+ + \cdots + (n-\alpha+1)_+] \\ & +(n-u) + (n-u-1) + (n-u-2)_+ + \cdots + (n-u-\alpha+1)_+.\end{aligned}$$

In both cases we get the result of the proposition. □

Remark 6. Putting $\alpha = 1$ in the proposition above yields [12, Proposition 1].

We can also obtain the analogue to [12, Theorem 1], which was already stated in [5, Remark 4.4].

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

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

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

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

We also have the following result (cf. [12, Section 2]).

Proposition 2. *We have*

$$\dim(\mathscr{C}) \leq m \quad \textit{and} \quad \dim(\mathcal{N}) \geq sn - m.$$

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

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., [10]), 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 $\mathbf{x}_{0,1}, \ldots, \mathbf{x}_{q^{m_1}-1,1}$ and the points of P_2 by $\mathbf{x}_{0,2}, \ldots, \mathbf{x}_{q^{m_2}-1,2}$. 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 q^m points

$$(\mathbf{x}_{i_1,1}, \mathbf{x}_{i_2,2}), \quad 0 \le i_1 \le q^{m_1} - 1, 0 \le i_2 \le q^{m_2} - 1.$$

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

$$D_j = \begin{pmatrix} C_{j,1} & \mathbf{0}^{n_1 \times m_2} \\ \mathbf{0}^{n_2 \times m_1} & \mathbf{0}^{n_2 \times m_2} \end{pmatrix}, \quad 1 \le j \le s_1,$$

and

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

where $\mathbf{0}^{k \times l}$ 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 $\mathbf{d}_{j,i}$ for $1 \le j \le s$.

We have the following result (which is Propagation Rule 4 in [10]).

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 let P_2 be 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*

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

Proof. It is easily verified that $0 \le \beta \le \min(1, \alpha m/n)$. 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 $\nu_1, \ldots, \nu_s \ge 0$ and, for $1 \le j \le s$, let $1 \le i_{j,\nu_j} < i_{j,\nu_j - 1} < \cdots < i_{j,1} \le n$, with

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

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

$$i_{1,1} + \cdots + i_{1,\min\{\nu_1,\alpha\}} + \cdots + i_{s_1,1} + \cdots + i_{s_1,\min\{\nu_{s_1},\alpha\}} \le \beta_1 n_1 - t_1,$$
$$i_{s_1+1,1} + \cdots + i_{s_1+1,\min\{\nu_{s_1+1},\alpha\}} + \cdots + i_{s,1} + \cdots + i_{s,\min\{\nu_s,\alpha\}} \le \beta_2 n_2 - t_2,$$

and, since $\beta_1, \beta_2 \le 1$,

$$i_{j,1} \le n_1, \quad 1 \le j \le s_1, \text{ and } i_{j,1} \le n_2, \quad s_1 + 1 \le j \le s.$$

As a consequence, we have that the row vectors $\mathbf{d}_{j,i_{j,\nu_j}}, \ldots, \mathbf{d}_{j,i_{j,1}}$ are rows of the matrix

$$\begin{pmatrix} C_{j,1} & \mathbf{0}^{n_1 \times m_2} \end{pmatrix}$$

for each $j \in \{1, \ldots, s_1\}$. Similarly, the row vectors $\mathbf{d}_{j,i_{j,\nu_j}}, \ldots, \mathbf{d}_{j,i_{j,1}}$ are rows of the matrix

$$\begin{pmatrix} \mathbf{0}^{n_2 \times m_1} & C_{j-s_1,2} \end{pmatrix}$$

for each $j \in \{s_1 + 1, \ldots, s\}$, respectively.

Due to the assumptions made on the parameters of P_1 and P_2, it thus follows that the row vectors $\mathbf{d}_{1,i_{1,\nu_1}}, \ldots, \mathbf{d}_{1,i_{1,1}}, \ldots, \mathbf{d}_{s,i_{s,\nu_s}}, \ldots, \mathbf{d}_{s,i_{s,1}}$ are linearly independent, which completes the proof. □

Remark 7. 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 βn to be of order αm (see Theorem 1 or [5, Corollary 5.5]). Note that we view β and t as functions of α (see [5, 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., [2]). 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.

Again let 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

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

and

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

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 [2]; see [2, Corollary 5.1].

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 let P_2 be 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*

$$\alpha = \max\{\alpha_1, \alpha_2\}, \quad \beta = \min\{\beta_1, \beta_2\}, \quad t = \lfloor \beta n \rfloor - k.$$

Remark 8. Similar to Remark 7, one should use $\alpha_1 = \alpha_2$ in Theorem 5 in order to be able to obtain βn to be of order αm.

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 [11], which itself is a generalization of the matrix-product construction of codes in [3]. 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 [11] for (d, k, m, s)-systems, and then we provide a bound on the quality of digital nets obtained this way. As the construction method is the same, the proof method is also very similar (indeed, this subsection is to a large extent identical to [11, Sections 3 and 4]; for completeness we repeat the necessary results and definitions here). As in [11], we introduce some notation and definitions first.

Let us first introduce matrices which are non-singular by column (NSC matrices) [3]. Let A be an $M \times M$ matrix over a finite field $\mathbb{F}_q$. For $1 \le l \le M$, let A_l denote the matrix which consists of the first l rows of A. For $1 \le k_1 < \cdots < k_l \le M$, 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 $1 \le l \le M$ and $1 \le k_1 < \cdots < k_l \le M$.

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

Remark 9. As noted in [11], an $M \times M$ NSC matrix over $\mathbb{F}_q$ exists if and only if $1 \le M \le q$; see [3, Section 3]. For any integer $1 \le M \le q$, an explicit $M \times M$ upper triangular NSC matrix over $\mathbb{F}_q$ is given in [3, Section 5.2].

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

Definition 5. Let $1 \le r_1 \le \cdots \le r_M$ 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 $1 \le l \le M$ and any $\mathbf{v}_l \in V_l$, let $\bar{\mathbf{v}}_l \in \mathbb{F}_q^r$ 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 $\bar{\mathbf{u}}_1, \ldots, \bar{\mathbf{u}}_M \in \mathbb{F}_q^r$ with

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

and

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

we have $\bar{u}_{k,l} = 0$ for each $1 \le l \le M$ and $r_l < k \le r$.

The following remark and lemma are from [11].

Remark 10. For any integers $1 \le r_1 \le \cdots \le r_M$, 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 $1 \le r_1 \le \cdots \le r_M$, A is compatible with $(\mathbb{F}_q^{r_1}, \ldots, \mathbb{F}_q^{r_M})$.*

Now we can 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 $C_{1,k}, \ldots, C_{s_k,k}$, $1 \le k \le M$, where we assume that $1 \le s_1 \le \cdots \le s_M$. Note that we now use the same value of α for all M digital nets; i.e., we assume that t_k and β_k are known for the same given value of α 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 $1 \le k \le M$ we form the matrices

$$C_k = ((C'_{1,k})^\top \mid \cdots \mid (C'_{s_k,k})^\top).$$

The row space of C_k is denoted by $\mathscr{C}_k \subseteq \mathbb{F}_q^{ns_k}$ and the dual space of $\mathscr{C}_k$ is denoted by $\mathscr{C}_k^\perp \subseteq \mathbb{F}_q^{ns_k}$.

Put $s = s_M$ and for each $k = 1, \ldots, M$ and $\mathbf{a}_k \in \mathscr{C}_k^\perp$, let $\bar{\mathbf{a}}_k \in \mathbb{F}_q^{ns}$ be the vector obtained from $\mathbf{a}_k \in \mathbb{F}_q^{ns_k}$ by appending enough zeroes, that is,

$$\bar{\mathbf{a}}_k^\top = \begin{pmatrix} \mathbf{a}_k^\top \\ \mathbf{0} \end{pmatrix} = \begin{pmatrix} \mathbf{a}_{1,k}^\top \\ \vdots \\ \mathbf{a}_{s_k,k}^\top \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

where $\mathbf{a}_{j,k} \in \mathbb{F}_q^n$ for $1 \le k \le M$ and $1 \le j \le s_k$.

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 $(\mathscr{C}_1^\perp, \ldots, \mathscr{C}_M^\perp)$ (this of course implies that $M \le q$). For example, we can choose an upper triangular NSC matrix as A.

Let

$$\overline{\mathcal{M}} := \{(\bar{\mathbf{a}}_1^\top \bar{\mathbf{a}}_2^\top \ldots \bar{\mathbf{a}}_M^\top) \cdot A : \mathbf{a}_k \in \mathscr{C}_k^\perp \text{ for } 1 \le k \le M\};$$

i.e., $\overline{\mathcal{M}}$ 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

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

Let

$$\overline{C} = (\bar{\mathbf{c}}_1^\top \bar{\mathbf{c}}_2^\top \ldots \bar{\mathbf{c}}_M^\top) \in \overline{\mathcal{M}}$$

be a matrix in $\overline{\mathcal{M}}$, where

$$\bar{\mathbf{c}}_k^\top = \begin{pmatrix} \bar{\mathbf{c}}_{1,k}^\top \\ \bar{\mathbf{c}}_{2,k}^\top \\ \vdots \\ \bar{\mathbf{c}}_{s,k}^\top \end{pmatrix}$$

and $\bar{\mathbf{c}}_{j,k} \in \mathbb{F}_q^n$ for $1 \le k \le M$ and $1 \le j \le s$. Since A is invertible, there exist uniquely determined vectors $\mathbf{a}_1 \in \mathscr{C}_1^\perp, \ldots, \mathbf{a}_M \in \mathscr{C}_M^\perp$, such that

$$(\bar{\mathbf{c}}_1^\top \ldots \bar{\mathbf{c}}_M^\top) = (\bar{\mathbf{a}}_1^\top \ldots \bar{\mathbf{a}}_M^\top) \cdot A. \tag{4}$$

Note that for $1 \le k \le M$ we have

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

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

$$\bar{\mathbf{c}}_{j,k}^\top = \sum_{v=1}^{M} \bar{\mathbf{a}}_{j,v}^\top A_{v,k} \tag{5}$$

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

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

Since A is compatible with $(\mathscr{C}_1^\perp, \dots, \mathscr{C}_M^\perp)$, we have

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

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

$$C = (\mathbf{c}_1 \mathbf{c}_2 \dots \mathbf{c}_M).$$

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

Let $\mathcal{N} = \phi(\overline{\mathcal{M}})$. Let $C = (\mathbf{c}_1 \dots \mathbf{c}_M) \in \mathcal{N}$ be a vector, where for each $1 \le k \le M$ we have $\mathbf{c}_k \in \mathbb{F}_q^{ns_k}$ with

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

and $\mathbf{c}_{j,k} \in \mathbb{F}_q^n$ for $1 \le j \le s_k$. 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 $n = \max_{1 \le k \le M} n_k$ (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 Lemma 1).

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

$$\mu_{\alpha,n}(C) = \sum_{k=1}^{M} \mu_{\alpha,n}(\mathbf{c}_k) = \sum_{k=1}^{M} \sum_{j=1}^{s_k} \mu_\alpha(\mathbf{c}_{j,k}).$$

We have $C = (\mathbf{c}_1 \dots \mathbf{c}_M) \in \mathbb{F}_q^{n(s_1+\cdots+s_M)}$ and assume that $C \ne \mathbf{0}$. By the definition of C, there are vectors $\mathbf{a}_1 \in \mathscr{C}_1^\perp, \dots, \mathbf{a}_M \in \mathscr{C}_M^\perp$ such that

$$(\bar{\mathbf{c}}_1^\top \dots \bar{\mathbf{c}}_M^\top) = (\bar{\mathbf{a}}_1^\top \dots \bar{\mathbf{a}}_M^\top) \cdot A.$$

Let l be the largest integer such that $\mathbf{a}_l \ne \mathbf{0}$ (this exists as $C \ne \mathbf{0}$). Note that

$$\mathbf{a}_l^\top = \begin{pmatrix} \mathbf{a}_{1,l}^\top \\ \vdots \\ \mathbf{a}_{s_l,l}^\top \end{pmatrix}$$

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

The following lemma is a generalization of [11, Lemma 4.1].

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

$$\mu_\alpha(\bar{\mathbf{c}}_{j,1}) + \cdots + \mu_\alpha(\bar{\mathbf{c}}_{j,M}) \geq (M - l + 1)\mu_\alpha(\mathbf{a}_{j,l}).$$

Proof. Let $j \in \{j_1, \dots, j_u\}$, and let $\bar{\mathbf{a}}_{j,l} = (a_{j,l,1} \dots a_{j,l,n})$. 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 $i \in \{1, \dots, n\} \setminus \{i_{j,l,1}, \dots, i_{j,l,v}\}$. Then $\mu_\alpha(\mathbf{a}_{j,l}) = \mu_\alpha(\bar{\mathbf{a}}_{j,l}) = i_{j,l,1} + \cdots + i_{j,l,\min(v,\alpha)}$. Let $i \in \{i_{j,l,1}, \dots, i_{j,l,\min(v,\alpha)}\}$.

Let the ith entries of $\bar{\mathbf{a}}_{j,1}, \dots, \bar{\mathbf{a}}_{j,M} \in \mathbb{F}_q^n$ be given by $\alpha_1, \dots, \alpha_M \in \mathbb{F}_q$, and let the ith entries of $\bar{\mathbf{c}}_{j,1}, \dots, \bar{\mathbf{c}}_{j,M} \in \mathbb{F}_q^n$ be given by $\beta_1, \dots, \beta_M \in \mathbb{F}_q$. By (4) we have

$$(\beta_1 \dots \beta_M) = (\alpha_1 \dots \alpha_M) \cdot A. \tag{6}$$

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

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

In the following we show that there are at least $M - l + 1$ entries of $(\beta_1 \dots \beta_M)$ 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

$$\mathbf{0} = (\beta_{k_1} \dots \beta_{k_l}) = (\alpha_1 \dots \alpha_l) \cdot A(k_1, \dots, k_l).$$

But as $\alpha_l \neq 0$ and $A(k_1, \dots, k_l)$ is non-singular (as A is NSC) it follows that $(\beta_{k_1} \dots \beta_{k_l}) \neq \mathbf{0}$, which yields a contradiction. Hence there are at least $M - l + 1$ entries of $(\beta_1 \dots \beta_M)$ which are non-zero. As this holds for all $i \in \{i_{j,l,1}, \dots, i_{j,l,\min(v,\alpha)}\}$, the result follows. □

The following lemma is a generalization of [11, Lemma 4.2].

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

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

Proof. We have $\mu_{\alpha,n}(C) = \sum_{k=1}^{M} \sum_{j=1}^{s_k} \mu_\alpha(\mathbf{c}_{j,k})$ and $\mu_{\alpha,n}(\mathbf{a}_l) = \mu_\alpha(\mathbf{a}_{j_1,l}) + \cdots + \mu_\alpha(\mathbf{a}_{j_u,l})$. Since A is compatible with $(\mathscr{C}_1^\perp, \dots, \mathscr{C}_M^\perp)$, we have $\bar{\mathbf{c}}_{j,k} = \mathbf{0} \in \mathbb{F}_q^n$ for any $1 \leq k \leq M$ and $s_k < j \leq s$. Therefore, for each $1 \leq k \leq M$ we have

$$\sum_{j=1}^{s_k} \mu_\alpha(\mathbf{c}_{j,k}) = \sum_{j=1}^{s} \mu_\alpha(\bar{\mathbf{c}}_{j,k}).$$

Hence

$$\mu_{\alpha,n}(C) = \sum_{k=1}^{M} \sum_{j=1}^{s} \mu_\alpha(\bar{\mathbf{c}}_{j,k}) = \sum_{j=1}^{s} \sum_{k=1}^{M} \mu_\alpha(\bar{\mathbf{c}}_{j,k}) \geq \sum_{j \in \{j_1, \dots, j_u\}} \sum_{k=1}^{M} \mu_\alpha(\bar{\mathbf{c}}_{j,k}).$$

Lemma 2 now implies that

$$\mu_{\alpha,n}(C) \geq (M - l + 1) \sum_{j \in \{j_1, \dots, j_u\}} \mu_\alpha(\mathbf{a}_{j,l}) = (M - l + 1)\mu_{\alpha,n}(\mathbf{a}_l).$$

□

The following lemma is a generalization of [11, Theorem 4.3].

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

$$\delta_{\alpha,n}(\mathcal{N}) \geq \min_{1\leq l\leq M} (M-l+1)\delta_{\alpha,n}(\mathscr{C}_l^{\perp}).$$

Proof. By the construction of $\mathcal{N}$ we have $\dim \mathcal{N} = \sum_{k=1}^{M} \dim \mathscr{C}_k^{\perp}$. Since $\dim \mathscr{C}_k^{\perp} \geq ns_k - m_k$ the first result follows. The second result follows directly from Lemma 3. □

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 N' be a generating matrix for $\mathcal{N}^{\perp}$ and let m' be the number of rows of 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 N' to obtain a matrix N which generates $\mathcal{N}$ and has $m = m_1 + \cdots + m_M$ rows.

We partition N into submatrices $N_1, \ldots, N_{s_1+\cdots+s_M}$, each of size $m \times n$,

$$N = (N_1 \mid N_2 \mid \ldots \mid N_{s_1+\cdots+s_M}).$$

Then we define the generating matrices of the digital net by

$$D_j = N_j^{\top} \quad \text{for } 1 \leq j \leq s_1 + \cdots + s_M. \tag{7}$$

Remark 11. 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 and 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 $A_{l,l}$ are all non-zero and therefore have an inverse $A_{l,l}^{-1}$ 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 $C'_{j,k} \in \mathbb{F}_q^{n\times m_k}$ and let $\mathbf{0}^{n\times m}$ 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

$$D_j = \begin{pmatrix} \mathbf{0}^{n\times m_1} & \ldots & \mathbf{0}^{n\times m_{k-1}} & V_{k,k}C'_{j-\sigma_{k-1},k} & \ldots & V_{k,M}C'_{j-\sigma_{k-1},M} \end{pmatrix} \in \mathbb{F}_q^{n\times m},$$

where $V_{k,l} \in \mathbb{F}_q$ is given by $V_{k,k} = A_{k,k}^{-1}$ for $1 \leq k \leq M$, and for $l = 1, \ldots, M-1$ we set

$$V_{k,k+l} = -A_{k,k}^{-1}(A_{k,k+l}V_{k+l,k+l} + \cdots + A_{k,k+1}V_{k+1,k+l}) \quad \text{for } 1 \leq k \leq M-l;$$

i.e., the matrix $V = (V_{k,l})_{1\leq k,l\leq M}$, where $V_{k,l} = 0$ for $k > l$, is the inverse of A. The matrices $D_1, \ldots, D_{\sigma_M}$ are then the generating matrices of the digital net which has dual space $\mathcal{N}$.

The following theorem is a generalization of [11, Corollary 4.6].

Theorem 6 (Propagation Rule IX)**.** *Assume we are given digital $(t_k, \alpha, \beta_k, n_k\times m_k, s_k)$-nets (where $\beta_k n_k$ is an integer), $1 \leq k \leq M$, 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 $s = s_1 + \cdots + s_M$,

$n = \max_{1\le k\le M} n_k$, 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

$$t = \beta n + 1 - \min_{1\le l\le M}(M - l + 1)(\beta_l n_l - t_l + 1).$$

Proof. In view of Remark 3 we only need to prove a bound on $\beta n - t$ and choose β 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 $\delta_{\alpha,n}(\mathcal{N}) \ge \min_{1\le l\le M}(M - l + 1)\delta_{\alpha,n}(\mathscr{C}_l^\perp)$ and from Theorem 3 we obtain $\delta_{\alpha,n}(\mathscr{C}_k^\perp) \ge \beta_k n_k - t_k + 1$ for $1 \le k \le M$. Therefore $\delta_{\alpha,n}(\mathcal{N}) \ge \min_{1\le l\le M}(M - l + 1)(\beta_k n_k - t_k + 1)$. This implies that the linear independence condition in Definition 2 is satisfied if we choose t such that $\beta n - t + 1 = \delta_{\alpha,n}(\mathcal{N})$, i.e., $t = \beta n + 1 - \min_{1\le l\le M}(M - l + 1)(\beta_l n_l - t_l + 1)$. 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, $1 \le k \le M$, i.e., the α-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 $\mathbf{0}$. Then $D'_j \in \mathbb{F}_q^{n'\times m}$ for $1 \le j \le s_1 + \cdots + s_M$. 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 (where $\beta_k n_k$ is an integer), $1 \le k \le M$, 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 $\alpha' = \max_{1\le k\le M} \alpha_k$, $\beta' = \min_{1\le k\le M} \beta_k$ and

$$t' = \lfloor \beta' n' \rfloor + 1 - \min_{1\le l\le M}(M - l + 1)(\beta_l n_l - t_l + 1).$$

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

$$\beta' n' = \beta' n_1 + \cdots + \beta' n_M \le \beta_1 n_1 + \cdots + \beta_M n_M \le \alpha_1 m_1 + \cdots + \alpha_M m_M \le \alpha' m.$$

As $\alpha \ge \alpha_k$ we have $\delta_{\alpha,n}(\mathscr{C}_k^\perp) \ge \delta_{\alpha_k,n}(\mathscr{C}_k^\perp) \ge \beta_k n_k - t_k$ for $1 \le k \le M$. Thus, using the same arguments as in the proof of Theorem 6, the result follows by using Lemma 4. □

Remark 12. 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 11, augmented with enough rows of zeroes, are the same as in Section 3.2.

Remark 13. Although β 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 14. Similar to Remark 7, one should use $\alpha_1 = \cdots = \alpha_M$ in Corollary 1 in order to be able to obtain βn to be of order αm.

3.4. **A double m construction.** In [12], 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

$$D_j = \begin{pmatrix} C_{j,2} & C_{j,1} \\ -C_{j,2} & \mathbf{0}^{n\times m} \end{pmatrix}, \quad \text{for } 1 \le j \le s. \tag{8}$$

In [12], the construction is described via the dual space, which we repeat in the following. As in the previous sections, for $k = 1, 2$, we form the matrices

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

The row space of C_k is denoted by $\mathscr{C}_k \subseteq \mathbb{F}_q^{ns}$ and the dual space of $\mathscr{C}_k$ is denoted by $\mathscr{C}_k^\perp \subseteq \mathbb{F}_q^{ns}$. For $k = 1, 2$, let $\mathbf{a}_k = (\mathbf{a}_{1,k} \ldots \mathbf{a}_{s,k}) \in \mathscr{C}_k^\perp$ and set

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

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

$$\mathcal{N} = \{\mathbf{c} \in \mathbb{F}_q^{2ns} : \mathbf{a}_1 \in \mathscr{C}_1^\perp, \mathbf{a}_2 \in \mathscr{C}_2^\perp\}.$$

We have

$$\dim(\mathcal{N}) = \dim(\mathscr{C}_1^\perp) + \dim(\mathscr{C}_2^\perp) \ge 2(sn - m),$$

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

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

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

$$D(\mathscr{C}_1^\perp, \mathscr{C}_2^\perp) = \max_{1\le j\le s} \max_{R_j} \max(0, \mu_{\alpha,n}(\mathbf{a}_{j,1}) - \mu_{\alpha,n}(\mathbf{a}_{j,1} + \mathbf{a}_{j,2})),$$

where R_j is the set of all ordered pairs $(\mathbf{a}_1, \mathbf{a}_2)$, with $\mathbf{a}_k = (\mathbf{a}_{1,k} \ldots \mathbf{a}_{s,k}) \in \mathscr{C}_k^\perp \setminus \{\mathbf{0}\}$, $\mathbf{a}_{i,1} + \mathbf{a}_{i,2} = \mathbf{0}$ for $i \ne j$ and $\mathbf{a}_{j,1} + \mathbf{a}_{j,2} \ne \mathbf{0}$. We define the maximum over R_j to be zero if R_j is empty.

The following theorem generalizes [12, Theorem 5] (the proof is very similar to the proof of [12, Theorem 5]).

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

$$t \le \max(2\beta n - (1 + \beta_1)n + t_1 + D(\mathscr{C}_1^\perp, \mathscr{C}_2^\perp), 2\beta n - (1 + \beta_2)n + t_2, 0)$$

if $\mathscr{C}_1^\perp \cap \mathscr{C}_2^\perp = \{\mathbf{0}\}$, *and*

$$t \le \max(2\beta n - (1+\beta_1)n + t_1 + D(\mathscr{C}_1^\perp, \mathscr{C}_2^\perp), 2\beta n - (1+\beta_2)n + t_2, \\ 2\beta n + 1 - \delta_{\alpha,n}(\mathscr{C}_1^\perp \cap \mathscr{C}_2^\perp), 0)$$

if $\mathscr{C}_1^\perp \cap \mathscr{C}_2^\perp \neq \{\mathbf{0}\}$.

Proof. By the definition of α and β it follows that $0 < \beta \le 1$ and $2\beta n \le \beta_1 n + \beta_2 n \le \alpha_1 m + \alpha_2 m \le 2\alpha m$. Hence the parameters α and β 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 $\delta_{\alpha,2n}(\mathcal{N})$. Hence we only need to show a lower bound on $\mu_{\alpha,2n}(\mathbf{c})$ for all nonzero vectors $\mathbf{c}$ in $\mathcal{N}$.

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

Let $\mathbf{c} \in \mathcal{N}$ be nonzero. Then

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

We consider several cases. If $\mathbf{a}_1 = \mathbf{0}$, then $\mathbf{a}_2 \neq \mathbf{0}$ and therefore

$$\mu_{\alpha,2n}(\mathbf{c}) \ge n + \sum_{j=1}^{s} \mu_\alpha(\mathbf{a}_{j,2}) \ge n + \delta_{\alpha,n}(\mathscr{C}_2^\perp) \ge n + \beta_2 n - t_2 + 1.$$

If $\mathbf{a}_2 = \mathbf{0}$, then $\mathbf{a}_1 \neq \mathbf{0}$ and analogously we obtain

$$\mu_{\alpha,2n}(\mathbf{c}) \ge n + \sum_{j=1}^{s} \mu_\alpha(\mathbf{a}_{j,1}) \ge n + \delta_{\alpha,n}(\mathscr{C}_1^\perp) \ge n + \beta_1 n - t_1 + 1.$$

If $\mathbf{a}_1, \mathbf{a}_2 \neq \mathbf{0}$, but $\mathbf{a}_1 + \mathbf{a}_2 = \mathbf{0}$, then $\mathbf{a}_1 \in \mathscr{C}_1^\perp \cap \mathscr{C}_2^\perp$. If $\mathscr{C}_1^\perp \cap \mathscr{C}_2^\perp = \{\mathbf{0}\}$, then this case is not possible. If $\mathscr{C}_1^\perp \cap \mathscr{C}_2^\perp \neq \{\mathbf{0}\}$, then

$$\mu_{\alpha,2n}(\mathbf{c}) = \mu_{\alpha,n}(\mathbf{a}_1) \ge \delta_{\alpha,n}(\mathscr{C}_1^\perp \cap \mathscr{C}_2^\perp).$$

The last case is where $\mathbf{a}_1, \mathbf{a}_2 \neq \mathbf{0}$ and $\mathbf{a}_1 + \mathbf{a}_2 \neq \mathbf{0}$. Then

$$\mu_{\alpha,2n}(\mathbf{c}) \ge \sum_{\substack{j=1 \\ \mathbf{a}_{j,1}+\mathbf{a}_{j,2}\neq\mathbf{0}}}^{s} (n + \mu_\alpha(\mathbf{a}_{j,1} + \mathbf{a}_{j,2})) + \sum_{\substack{j=1 \\ \mathbf{a}_{j,1}+\mathbf{a}_{j,2}=\mathbf{0}}}^{s} \mu_\alpha(\mathbf{a}_{j,1}).$$

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

$$\begin{aligned} \mu_{\alpha,2n}(\mathbf{c}) &\ge n + \mu_\alpha(\mathbf{a}_{j_0,1} + \mathbf{a}_{j_0,2}) + \sum_{\substack{j=1 \\ j\neq j_0}}^{s} \mu_\alpha(\mathbf{a}_{j,1}) \\ &= n + \mu_{\alpha,n}(\mathbf{a}_1) + \mu_\alpha(\mathbf{a}_{j_0,1} + \mathbf{a}_{j_0,2}) - \mu_\alpha(\mathbf{a}_{j_0,1}) \\ &\ge n + \beta_1 n - t_1 + 1 - D(\mathscr{C}_1^\perp, \mathscr{C}_2^\perp). \end{aligned}$$

Therefore we have

$$\delta_{\alpha,2n}(\mathcal{N}) \ge \min((1+\beta_1)n - t_1 + 1 - D(\mathscr{C}_1^\perp, \mathscr{C}_2^\perp), (1+\beta_2)n - t_2 + 1)$$

if $\mathscr{C}_1^\perp \cap \mathscr{C}_2^\perp = \{\mathbf{0}\}$, and

$$\delta_{\alpha,2n}(\mathcal{N}) \ge \min((1+\beta_1)n - t_1 + 1 - D(\mathscr{C}_1^\perp, \mathscr{C}_2^\perp), (1+\beta_2)n - t_2 + 1, \delta_{\alpha,n}(\mathscr{C}_1^\perp \cap \mathscr{C}_2^\perp))$$

if $\mathscr{C}_1^\perp \cap \mathscr{C}_2^\perp \neq \{\mathbf{0}\}$. Thus the result follows. □

Remark 15. Similar to Remark 7, one should use $\alpha_1 = \alpha_2$ in Theorem 7 in order to be able to obtain βn to be of order αm.

3.5. **A base change propagation rule.** We state a result that is analogous to Theorem 9 in [13], which is sometimes also referred to as the trace code for digital nets (cf. [15]).

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 $\mathbb{F}_{q^r}$, 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 flavor as the proof of Theorem 9 in [13]. Let P be a digital $(t, \alpha, \beta, n \times m, s)$-net over $\mathbb{F}_{q^r}$, with generating matrices $C_1, \dots, C_s$, where each matrix C_j, $1 \le j \le s$ has row vectors $\mathbf{c}_{1,j}, \dots, \mathbf{c}_{n,j}$. We now choose an ordered basis $B_1, \dots, B_r$ of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$ and an $\mathbb{F}_q$-linear isomorphism $\varphi : \mathbb{F}_{q^r}^m \to \mathbb{F}_q^{rm}$. Then we consider the generating matrices of a net Q,

$$D_{(j-1)r+k} := \begin{pmatrix} \mathbf{d}_{1,(j-1)r+k} \\ \vdots \\ \mathbf{d}_{n,(j-1)r+k} \end{pmatrix}, \quad 1 \le j \le s, \ 1 \le k \le r,$$

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

Choose integers

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

such that

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

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

$$\sum_{j=1}^{s} \sum_{k=1}^{r} \sum_{l=1}^{\nu_{(j-1)r+k}} \delta_l^{(j,k)} \mathbf{d}_{i_{(j-1)r+k,l},(j-1)r+k} = \mathbf{0} \in \mathbb{F}_q^{rm}. \tag{9}$$

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

$$\sum_{j=1}^{s} \sum_{k=1}^{r} \sum_{l=1}^{\nu_{(j-1)r+k}} \delta_l^{(j,k)} \varphi\left(B_k \mathbf{c}_{i_{(j-1)r+k,l},j}\right) = \mathbf{0} \in \mathbb{F}_q^{rm}. \tag{10}$$

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

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

Furthermore, for $1 \le j \le s$ and $1 \le k \le r$, put $e_l^{(j,k)} = 1$ if

$$l \in \left\{ i_{(j-1)r+k,1}, \dots, i_{(j-1)r+k,\nu_{(j-1)r+k}} \right\}$$

and $e_l^{(j,k)} = 0$ otherwise. Then (10) can be rewritten as

$$\sum_{j=1}^{s} \sum_{k=1}^{r} \sum_{l \in U_j} e_l^{(j,k)} \delta_l^{(j,k)} \varphi\left(B_k \mathbf{c}_{i_{(j-1)r+k,l},j}\right) = \mathbf{0} \in \mathbb{F}_q^{rm}.$$

Since φ is an $\mathbb{F}_q$-linear isomorphism, we conclude that

$$\sum_{j=1}^{s} \sum_{l \in U_j} \gamma_l^{(j)} \mathbf{c}_{l,j} = \mathbf{0} \in \mathbb{F}_{q^r}^m$$

with

$$\gamma_l^{(j)} = \sum_{k=1}^{r} e_l^{(j,k)} \delta_l^{(j,k)} B_k \in \mathbb{F}_{q^r}. \tag{11}$$

Let us now consider

$$\sum_{j=1}^{s} \sum_{l \in U_j} \gamma_l^{(j)} \mathbf{c}_{l,j}.$$

For $1 \le j \le s$, 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 $1 \le g_{j,\mu_j}$ and $g_{j,1} \le n$, and $\sum_{j=1}^{s} \left(g_{j,1} + \cdots + g_{j,\min\{\mu_j,\alpha\}} \right) \le \beta n - t$, 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 $\mathbf{c}_{l,j}$ 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 $l \in U_j$, $1 \le j \le s$. Hence, by (11), $e_l^{(j,k)} \delta_l^{(j,k)} = 0$ for $l \in U_j$, $1 \le j \le s$, and $1 \le k \le r$. By the definition of the numbers $e_l^{(j,k)}$, all coefficients $\delta_l^{(j,k)}$ in (9) are zero. □

Remark 16. As in [13, 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 [14], where we change the ground field from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$, for some prime power q and some positive integer r. The difference to the previous propagation rule is that the $\mathbb{F}_q$-linear transformation from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q^r$ is now applied to the dual space instead of applying it to the generating matrices. The following result generalizes [14, Corollary 1].

Theorem 9 (Propagation Rule XII)**.** *Given a digital $(t, \alpha, \beta, n \times m, s)$-net over $\mathbb{F}_{q^r}$, we can construct a digital $(t', \alpha, \beta, rn \times rm, s)$-net over $\mathbb{F}_q$, where*

$$t' \le rt + (r-1)(s\alpha - 1).$$

Proof. Let $\varphi : \mathbb{F}_{q^r} \to \mathbb{F}_q^r$ denote again an $\mathbb{F}_q$-linear isomorphism. Let $C_1, \ldots, C_s \in \mathbb{F}_{q^r}^{n \times m}$ denote the generating matrices of the digital $(t, \alpha, \beta, n \times m, s)$-net, and let $C = (C_1^\top \mid \cdots \mid C_s^\top)$. The row space of C is denoted by $\mathscr{C} \subseteq \mathbb{F}_{q^r}^{sn}$, and the dual space of $\mathscr{C}$ is denoted by $\mathscr{C}^\perp \subseteq \mathbb{F}_{q^r}^{sn}$. For a vector $\mathbf{c} = (\mathbf{c}_1, \ldots, \mathbf{c}_s) \in \mathscr{C}^\perp$, with $\mathbf{c}_j \in \mathbb{F}_{q^r}^n$, let $\bar{\mathbf{c}}_j = \varphi(\mathbf{c}_j) \in \mathbb{F}_q^{rn}$ and $\bar{\mathbf{c}} = (\bar{\mathbf{c}}_1, \ldots, \bar{\mathbf{c}}_s)$, where we extend the $\mathbb{F}_q$-linear isomorphism from $\mathbb{F}_{q^r} \to \mathbb{F}_q^r$ componentwise, to an $\mathbb{F}_q$-linear isomorphism from $\mathbb{F}_{q^r}^n \to \mathbb{F}_q^{rn}$. Then we obtain a linear space $\bar{\mathscr{C}}^\perp \subseteq \mathbb{F}_q^{rsn}$, by setting $\bar{\mathscr{C}}^\perp = \{\bar{\mathbf{c}} : \mathbf{c} \in \mathscr{C}^\perp\}$.

Note that $\dim_{\mathbb{F}_q}(\bar{\mathscr{C}}^\perp) = r \dim_{\mathbb{F}_{q^r}}(\mathscr{C}^\perp)$, and $\dim_{\mathbb{F}_{q^r}}(\mathscr{C}^\perp) \ge sn - m$ by Proposition 2. Thus $\dim_{\mathbb{F}_q}(\bar{\mathscr{C}}^\perp) \ge rsn - rm$, and the dual space of $\bar{\mathscr{C}}^\perp$, denoted by $\bar{\mathscr{C}}$, satisfies $\dim_{\mathbb{F}_q}(\bar{\mathscr{C}}) \le rm$. Let $\bar{C} \in \mathbb{F}_q^{rm \times rsn}$ be a matrix whose row space is $\bar{\mathscr{C}}$, and let $\bar{C} = (D_1^\top \mid \cdots \mid D_s^\top)$, where $D_j \in \mathbb{F}_q^{rn \times rm}$ for $1 \le j \le s$. 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 $\bar{\mathbf{c}} \in \bar{\mathscr{C}}^{\perp}$ be a nonzero vector. We have $\mu_{\alpha,rn}(\bar{\mathbf{c}}) = \mu_\alpha(\bar{\mathbf{c}}_1) + \cdots + \mu_\alpha(\bar{\mathbf{c}}_s)$. As $\bar{\mathbf{c}}$ is nonzero, it follows that $\mathbf{c}$ is nonzero. If $\mu_\alpha(\mathbf{c}_j) = 0$, then $\mathbf{c}_j = \mathbf{0}$ and hence $\bar{\mathbf{c}}_j = \mathbf{0}$, which implies $\mu_\alpha(\bar{\mathbf{c}}_j) = 0$.

Let $\mu_\alpha(\mathbf{c}_j) > 0$, and $\mathbf{c}_j = (c_{j,1}, \ldots, c_{j,n})$. Let $i_{j,1} > \cdots > i_{j,\nu_j} > 0$ be the indices of the nonzero elements of $\mathbf{c}_j$, i.e., $c_{j,i_{j,v}} \neq 0$ for $1 \leq v \leq \nu_j$ and $c_{j,i} = 0$ for $i \notin \{i_{j,1}, \ldots, i_{j,\nu_j}\}$. Then $\bar{\mathbf{c}}_j = (\varphi(c_{j,1}), \ldots, \varphi(c_{j,n}))$, and $\varphi(c_{j,i_{j,v}}) \neq \mathbf{0}$ for $1 \leq v \leq \nu_j$, and $\varphi(c_{j,i}) = \mathbf{0}$, for $i \notin \{i_{j,1}, \ldots, i_{j,\nu_j}\}$. Then

$$\begin{aligned}
\mu_\alpha(\bar{\mathbf{c}}_j) &\geq \sum_{u=1}^{\min(\alpha,\nu_j)} (r(i_{j,u} - 1) + 1) \\
&= r \sum_{u=1}^{\min(\alpha,\nu_j)} i_{j,u} - (r-1)\min(\alpha, \nu_j) \\
&= r\mu_\alpha(\mathbf{c}_j) - (r-1)\alpha.
\end{aligned}$$

The above inequality also holds if $\mu_\alpha(\mathbf{c}_j) = 0$; hence

$$\begin{aligned}
\mu_{\alpha,rn}(\bar{\mathbf{c}}) &\geq \sum_{j=1}^{s} (r\mu_\alpha(\mathbf{c}_j) - (r-1)\alpha) \\
&= r\mu_{\alpha,n}(\mathbf{c}) - s(r-1)\alpha \geq r\delta_{\alpha,n}(\mathscr{C}^{\perp}) - s(r-1)\alpha.
\end{aligned}$$

As the last inequality holds for all nonzero $\bar{\mathbf{c}} \in \bar{\mathscr{C}}^{\perp}$, it follows that $\delta_{\alpha,rn}(\bar{\mathscr{C}}^{\perp}) \geq r\delta_{\alpha,n}(\mathscr{C}^{\perp}) - s(r-1)\alpha$. Thus we can choose t' such that $\beta rn - t' + 1 = \delta_{\alpha,rn}(\bar{\mathscr{C}}^{\perp})$. Using $\delta_{\alpha,n}(\mathscr{C}^{\perp}) \geq \beta n - t + 1$, 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 [15] under the name "base reduction for projective spaces". Let $r \geq 1$. Let $C_1, \ldots, C_s \in \mathbb{F}_{q^r}^{n \times m}$ 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 by some nonzero element in $\mathbb{F}_{q^r}$. Doing so, we can obtain generating matrices $C'_1, \ldots, C'_s \in \mathbb{F}_{q^r}^{n \times m}$, 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 φ be an $\mathbb{F}_q$-linear isomorphism from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q^r$ such that $\varphi(1) = (0, \ldots, 0, 1) \in \mathbb{F}_q^r$. For a vector $\mathbf{c} \in \mathbb{F}_{q^r}^m$ with $\mathbf{c} = (c_1, \ldots, c_m)$ we define $\varphi(\mathbf{c}) = (\varphi(c_1), \ldots, \varphi(c_m)) \in \mathbb{F}_q^{rm}$, and for a matrix $C \in \mathbb{F}_{q^r}^{n \times m}$ with $C = (\mathbf{c}_1^\top, \ldots, \mathbf{c}_n^\top)^\top$, we define $\varphi(C) = (\varphi(\mathbf{c}_1)^\top, \ldots, \varphi(\mathbf{c}_n)^\top)^\top \in \mathbb{F}_q^{n \times rm}$.

For $1 \leq j \leq s$, now let $D'_j = \varphi(C'_j) \in \mathbb{F}_q^{n \times rm}$. 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 $D_j \in \mathbb{F}_q^{n \times (rm-(r-1))}$ 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 $D'_1, \ldots, D'_s$ is the same as the strength of the digital net with generating 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 [5], 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 $C_j = (\mathbf{c}_{j,1}^\top, \ldots, \mathbf{c}_{j,n}^\top)^\top$ for $j = 1, \ldots, sd$, i.e., $\mathbf{c}_{j,l}$ is the lth row of C_j. Now let the matrix D_j be composed of the first rows of the matrices $C_{(j-1)d+1}, \ldots, C_{jd}$, then the second rows of $C_{(j-1)d+1}, \ldots, C_{jd}$, and so on. The matrix D_j is then a $dn \times m$ matrix, i.e., $D_j = ((\mathbf{d}_{j,1})^\top, \ldots, (\mathbf{d}_{j,dn})^\top)^\top$, where $\mathbf{d}_{j,l} = \mathbf{c}_{u,v}$ 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 [5, Theorem 4.11] (see also [4, Theorem 4.1] and [1, Theorem 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 $(t, \alpha, \beta, n \times m, sd)$-net over the finite field $\mathbb{F}_q$, where we assume that βn is an integer. 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

$$t' = \left\lceil \min(d, \alpha'/\alpha) \min\left(\beta n, t + \left\lfloor \frac{\alpha s(d-1)}{2} \right\rfloor\right)\right\rceil.$$

Proof. First note that if $\beta n \leq t + \lfloor \alpha s(d-1)/2 \rfloor$, then $t' = \min(d, \alpha'/\alpha)\beta n$ and

$$\beta \min(1, \alpha'/(\alpha d))dn - t' = \beta \min(d, \alpha'/\alpha)n - \beta \min(d, \alpha'/\alpha)n = 0;$$

hence in this case the bound is trivial.

Assume now that $\beta n > t + \lfloor \alpha s(d-1)/2 \rfloor$. Let $D_j = ((\mathbf{d}_{j,1})^\top, \ldots, (\mathbf{d}_{j,dn})^\top)^\top$ for $j = 1, \ldots, s$. Further, let the integers $i_{1,1}, \ldots, i_{1,\nu_1}, \ldots, i_{s,1}, \ldots, i_{s,\nu_s}$ be such that $1 \leq i_{j,\nu_j} < \cdots < i_{j,1} \leq dn$ and

$$i_{1,1} + \cdots + i_{1,\min(\nu_1,\alpha)} + \cdots + i_{s,1} + \cdots + i_{s,\min(\nu_s,\alpha)} \leq \beta \min(1, \alpha'/(\alpha d))dn - t'.$$

We need to show that the vectors

$$\mathbf{d}_{1,i_{1,1}}, \ldots, \mathbf{d}_{1,i_{1,\nu_1}}, \ldots, \mathbf{d}_{s,i_{s,1}}, \ldots, \mathbf{d}_{s,i_{s,\nu_s}}$$

are linearly independent over $\mathbb{F}_q$.

For $j = 1, \ldots, s$ let $U_j = \{\mathbf{d}_{j,i_{j,\nu_j}}, \ldots, \mathbf{d}_{j,i_{j,1}}\}$. 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 $\{(e_{f_j,u} - j)d + f_j : u = 1, \ldots, w_{f_j}\} \subseteq \{i_{j,\nu_j}, \ldots, i_{j,1}\}$, 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

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

Furthermore, we have

$$\begin{aligned}
&\sum_{f_j=(j-1)d+1}^{jd}\left(\sum_{r=1}^{\min(\alpha,w_{f_j})} d(e_{f_j,r}-1)+\min(\alpha,w_{f_j})(f_j-(j-1)d)\right)\\
&\quad=\sum_{f_j=(j-1)d+1}^{jd}\left(\sum_{r=1}^{\min(\alpha,w_{f_j})} de_{f_j,r}+\min(\alpha,w_{f_j})(f_j-jd)\right)\\
&\quad\geq\sum_{f_j=(j-1)d+1}^{jd}\sum_{r=1}^{\min(\alpha,w_{f_j})} de_{f_j,r}-\alpha\frac{d(d-1)}{2}. \qquad (12)
\end{aligned}$$

Thus

$$\begin{aligned}
d\sum_{j=1}^{s}\sum_{f_j=(j-1)d+1}^{jd}\sum_{r=1}^{\min(\alpha,w_{f_j})} e_{f_j,r} &\leq \sum_{j=1}^{s}(i_{j,1}+\cdots+i_{j,\min(\nu_j,\alpha')})+s\alpha\frac{d(d-1)}{2}\\
&\leq \beta\min(1,\alpha'/(\alpha d))dn-t'+s\alpha\frac{d(d-1)}{2}
\end{aligned}$$

and therefore

$$\begin{aligned}
\sum_{j=1}^{s}\sum_{f_j=(j-1)d+1}^{jd}\sum_{r=1}^{\min(\alpha,w_{f_j})} e_{f_j,r} &\leq \beta n-\frac{t'}{d}+s\alpha\frac{d-1}{2}\\
&\leq \beta n-t-\left\lfloor\frac{\alpha s(d-1)}{2}\right\rfloor+\frac{\alpha s(d-1)}{2}\\
&\leq \beta n-t+\frac{1}{2}.
\end{aligned}$$

As $e_{f_j,r}$, βn and t are all integers, it follows that

$$\sum_{j=1}^{s}\sum_{f_j=(j-1)d+1}^{jd}\sum_{r=1}^{\min(\alpha,w_{f_j})} e_{f_j,r}\leq\beta n-t.$$

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 $\mathbf{d}_{1,i_{1,1}},\ldots,\mathbf{d}_{1,i_{1,\nu_1}},\ldots,\mathbf{d}_{s,i_{s,1}},\ldots,\mathbf{d}_{s,i_{s,\nu_s}}$ are linearly independent.

Now let $\alpha d>\alpha'$. For a given $1\leq j\leq s$ with $\nu_j\geq\alpha'$ we have

$$\begin{aligned}
&\sum_{f_j=(j-1)d+1}^{jd}\left(\sum_{r=1}^{\min(\alpha,w_{f_j})} d(e_{f_j,r}-1)+\min(\alpha,w_{f_j})(f_j-(j-1)d)\right)\\
&\qquad\leq\quad i_{j,1}+\cdots+i_{j,\alpha'}+(\alpha d-\alpha')i_{j,\alpha'}
\end{aligned}$$

and for $1\leq j\leq s$ with $\nu_j<\alpha'$ we have

$$\begin{aligned}
&\sum_{f_j=(j-1)d+1}^{jd}\left(\sum_{r=1}^{\min(\alpha,w_{f_j})} d(e_{f_j,r}-1)+\min(\alpha,w_{f_j})(f_j-(j-1)d)\right)\\
&\qquad\leq\quad i_{j,1}+\cdots+i_{j,\nu_j}.
\end{aligned}$$

Note that

$$\sum_{j=1,\nu_j\geq\alpha'}^{s} i_{j,\alpha'} \leq \beta\min(1/\alpha',1/(\alpha d))dn - t'/\alpha'.$$

Let

$$I_j = \begin{cases} i_{j,1}+\cdots+i_{j,\min(\nu_j,\alpha')}+(\alpha d-\alpha')i_{j,\min(\nu_j,\alpha')} & \text{if } \nu_j\geq\alpha', \\ i_{j,1}+\cdots+i_{j,\min(\nu_j,\alpha')} & \text{if } \nu_j<\alpha'. \end{cases}$$

Hence we have

$$\begin{aligned}\sum_{j=1}^{s} I_j &\leq \beta\min(1,\alpha'/(\alpha d))dn - t' + (\alpha d-\alpha')(\beta\min(1/\alpha',1/(\alpha d))dn - t'/\alpha') \\ &= \beta\min(\alpha d/\alpha',1)dn - t'\alpha d/\alpha'.\end{aligned}$$

Further we can use inequality (12) again. Thus it follows that

$$\begin{aligned} d\sum_{j=1}^{s}\sum_{f_j=(j-1)d+1}^{jd}\sum_{r=1}^{\min(\alpha,w_{f_j})} e_{f_j,r} &\leq \sum_{j=1}^{s} I_j + s\alpha\frac{d(d-1)}{2} \\ &\leq \beta\min(\alpha d/\alpha',1)dn - t'\alpha d/\alpha' + s\alpha\frac{d(d-1)}{2}\end{aligned}$$

and therefore

$$\begin{aligned}\sum_{j=1}^{s}\sum_{f_j=(j-1)d+1}^{jd}\sum_{r=1}^{\min(\alpha,w_{f_j})} e_{f_j,r} &\leq \beta n - t'\frac{\alpha}{\alpha'} + s\alpha\frac{d-1}{2} \\ &\leq \beta n - t - \left\lfloor s\alpha\frac{d-1}{2}\right\rfloor + s\alpha\frac{d-1}{2} \\ &\leq \beta n - t + \frac{1}{2}.\end{aligned}$$

As $e_{f_j,r}$, βn and t are all integers, it follows that

$$\sum_{j=1}^{s}\sum_{f_j=(j-1)d+1}^{jd}\sum_{r=1}^{\min(\alpha,w_{f_j})} e_{f_j,r} \leq \beta n - t.$$

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 $\mathbf{d}_{1,i_{1,1}},\ldots,\mathbf{d}_{1,i_{1,\nu_1}},\ldots\ldots,\mathbf{d}_{s,i_{s,1}},\ldots,$ $\mathbf{d}_{s,i_{s,\nu_s}}$ are linearly independent, and hence the result follows. □

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 [1, 5].

In the tables below, 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 all tables we consider m between 15 and 30. Since α and β 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 3, 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 σ 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.

- σ_{dir}: The strength of a digital $(t, 2, 1, 2m \times m, s)$-net over $\mathbb{F}_q$ using the generating matrices of an existing classical digital $(t', m, 2s)$-net over $\mathbb{F}_q$, where we then obtain (cf. [1, 5])
$$t = 2 \min \left\{ m, t' + \left\lfloor \frac{s}{2} \right\rfloor \right\}.$$
(See also Theorem 11, which is a generalization of the result in [5]. Further, see [6] for constructions of polynomial lattice rules.) In the following we refer to this construction method as the direct construction method.
- σ_{VII}: The strength of a digital net constructed from a digital $(t_1, 2, 2m_1 \times m_1, s_1)$-net P_1 and a digital $(t_2, 2, 2m_2 \times m_2, s_2)$-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, $n = 2m$.
- σ_{VIII}: The strength of a digital net constructed from a digital $(t_1, 2, 2m_1 \times m_1, s_1)$-net P_1 and a digital $(t_2, 2, 2m_2 \times m_2, s_2)$-net P_2 $(s_1 \le s_2)$ 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, $n = 2m$.
- σ_{IX}: The strength of a digital net constructed from a digital $(t_1, 2, 2m_1 \times m_1, s_1)$-net P_1, a digital $(t_2, 2, 2m_2 \times m_2, s_2)$-net P_2, and a digital $(t_3, 2, 2m_3 \times m_3, s_3)$-net P_3 $(s_1 \le s_2 \le s_3)$ 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, $n = 2m$.
- σ_{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, σ_{XI} does not occur in the tables for dimension $s = 25$. For σ_{XI} we have $n = 2(m/3)$ (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 1. σ-values depending on m ($15 \le m \le 30$) for $\alpha = 2$, $\beta = 1$, $q = 2$, and $s = 15$ (left), $s = 25$ (right).

m	σ_{dir}	σ_{VII}	σ_{VIII}	σ_{XI}
15	0	0	1	4
16	0	0	1	
17	0	2	2	
18	0	2	2	6
19	2	2	2	
20	2	2	4	
21	2	4	4	8
22	2	4	5	
23	2	4	6	
24	2	4	6	10
25	4	6	8	
26	4	6	8	
27	6	6	9	12
28	8	8	10	
29	10	10	10	
30	12	12	12	14

m	σ_{dir}	σ_{VII}	σ_{VIII}
15	0	0	0
16	0	0	0
17	0	0	1
18	0	0	1
19	0	0	1
20	0	0	1
21	0	0	1
22	0	0	1
23	0	0	1
24	0	0	1
25	0	0	1
26	0	0	1
27	0	0	1
28	0	0	1
29	0	0	1
30	0	0	1

TABLE 2. σ-values depending on m ($15 \le m \le 30$) for $\alpha = 2$, $\beta = 1$, $q = 3$, and $s = 15$ (left), $s = 25$ (right).

m	σ_{dir}	σ_{VII}	σ_{VIII}	σ_{IX}	σ_{XI}
15	0	2	2	5	6
16	0	2	4	5	
17	0	2	4	6	
18	2	4	5	6	8
19	2	4	6	8	
20	4	4	6	8	
21	4	6	8	8	10
22	6	6	8	9	
23	6	6	9	10	
24	8	8	9	12	12
25	8	8	10	13	
26	10	10	12	13	
27	10	10	13	14	14
28	12	12	13	14	
29	14	14	14	16	
30	16	16	16	17	16

m	σ_{dir}	σ_{VII}	σ_{VIII}	σ_{IX}
15	0	0	1	1
16	0	0	1	1
17	0	0	1	2
18	0	0	1	2
19	0	0	1	2
20	0	0	1	2
21	0	0	1	2
22	0	0	1	2
23	0	0	1	2
24	0	0	1	4
25	0	0	1	4
26	0	2	2	5
27	0	2	2	5
28	0	2	2	6
29	0	2	2	6
30	0	2	4	8

- 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.

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

m	σ_{dir}	σ_{VII}	σ_{VIII}	σ_{IX}
15	0	4	5	6
16	2	4	5	8
17	2	4	6	8
18	4	6	8	9
19	4	6	9	10
20	6	6	10	12
21	8	8	12	13
22	8	8	13	14
23	10	10	13	14
24	12	12	14	16
25	14	14	16	17
26	16	16	17	18
27	18	18	18	20
28	20	20	20	20
29	22	22	22	22
30	24	24	24	24

m	σ_{dir}	σ_{VII}	σ_{VIII}	σ_{IX}
15	0	0	1	2
16	0	0	1	2
17	0	0	1	2
18	0	0	1	2
19	0	0	1	2
20	0	0	1	2
21	0	0	1	4
22	0	0	1	4
23	0	2	2	5
24	0	2	2	5
25	0	2	4	6
26	0	2	4	6
27	2	4	5	8
28	2	4	5	8
29	4	4	5	9
30	6	6	6	10

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous referee, 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

[1] Dick, J., Baldeaux, J.: Equidistribution properties of generalized nets and sequences. To apear in: L'Ecuyer, P. and Owen, A. (eds.): *Monte Carlo and Quasi-Monte Carlo Methods 2008*, 2010.

[2] Bierbrauer, J., Edel, Y., Schmid, W.Ch.: Coding-theoretic constructions for (t, m, s)-nets and ordered orthogonal arrays. J. Comb. Des. **10**, 403–418, 2002. MR1932120 (2003k:94047)

[3] Blackmore, N., Norton, G.H.: Matrix-product codes over $\mathbb{F}_q$. Applicable Algebra Engrg. Comm. Comput. **12**, 477-500, 2001. MR1873271 (2002m:94054)

[4] Dick, J.: Explicit constructions of quasi-Monte Carlo rules for the numerical integration of high-dimensional periodic functions. SIAM J. Numer. Anal. **45**, 2141–2176, 2007. MR2346374 (2008h:11076)

[5] Dick, J.: Walsh spaces containing smooth functions and quasi-Monte Carlo rules of arbitrary high order. SIAM J. Numer. Anal. **46**, 1519–1553, 2008. MR2391005 (2009d:42077)

[6] Dick, J., Kritzer, P., Pillichshammer, F., Schmid, W.Ch.: On the existence of higher order polynomial lattices based on a generalized figure of merit. J. Complexity **23**, 581–593, 2007. MR2372015 (2009a:65054)

[7] Niederreiter, H.: Point sets and sequences with small discrepancy. Monatsh. Math. **104**, 273-337, 1987. MR918037 (89c:11120)

[8] Niederreiter, H.: Random Number Generation and Quasi-Monte Carlo Methods, CBMS–NSF Series in Applied Mathematics 63, SIAM, Philadelphia, 1992. MR1172997 (93h:65008)

[9] Niederreiter, H.: Constructions of (t, m, s)-nets. In: Niederreiter, H. and Spanier. J. (eds.): *Monte Carlo and Quasi-Monte Carlo Methods 1998*. Springer, Berlin, 2000, pp. 70–85. MR1849843 (2002e:65012)

[10] Niederreiter, H.: Constructions of (t, m, s)-nets and (t, s)-sequences. Finite Fields Appl. **11**, 578–600, 2005. MR2158777 (2006c:11090)

[11] Niederreiter, H., Özbudak, F.: Matrix-product constructions of digital nets. Finite Fields Appl. **10**, 464–479, 2004. MR2067609 (2005f:11289)

[12] Niederreiter, H., Pirsic, G.: Duality for digital nets and its applications. Acta Arith. **97**, 173–182, 2001. MR1824983 (2001m:11130)

[13] Niederreiter, H., Xing, C.P.: Nets, (t, s)-sequences, and algebraic geometry. In: Hellekalek, P. and Larcher, G. (eds.): *Random and Quasi-Random Point Sets*. Springer, New York, 1998, pp. 267–302. MR1662844 (99k:11121)

[14] Niederreiter, H., Xing, C.P.: Constructions of digital nets. Acta Arith. **102**, 189–197, 2002. MR1889629 (2003a:11092)

[15] R. Schürer, W.Ch. Schmid: *MinT—the database of optimal net, code, OA, and OOA parameters*. Available at: `http://mint.sbg.ac.at` (February 2, 2010).

School of Mathematics and Statistics, The University of New South Wales, Sydney 2052, Australia

E-mail address: `josef.dick@unsw.edu.au`

School of Mathematics and Statistics, The University of New South Wales, Sydney 2052, Australia

E-mail address: `peter.kritzer@gmail.com`