<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>Some constructions of $(t, m, s)$-nets with improved parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Ling, San; Özbudak, Ferruh</td>
</tr>
<tr>
<td><strong>Citation</strong></td>
<td>Ling, S., &amp; Özbudak, F. (2007). Some constructions of $(t, m, s)$-nets with improved parameters. Finite Fields and Their Applications, 14(3), 658-675.</td>
</tr>
<tr>
<td><strong>Date</strong></td>
<td>2007</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="http://hdl.handle.net/10220/9853">http://hdl.handle.net/10220/9853</a></td>
</tr>
<tr>
<td><strong>Rights</strong></td>
<td>© 2007 Elsevier Inc. This is the author created version of a work that has been peer reviewed and accepted for publication by Finite Fields and Their Applications, Elsevier Inc. It incorporates referee’s comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [<a href="http://dx.doi.org/10.1016/j.ffa.2007.09.007">http://dx.doi.org/10.1016/j.ffa.2007.09.007</a>].</td>
</tr>
</tbody>
</table>
Some constructions of \((t, m, s)\)-nets with improved parameters

San Ling\(^a\), Ferruh Özbudak\(^{a, b, *}\)

\(^a\) Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Block 5 Level 3, 1 Nanyang Walk, Singapore 637616, Republic of Singapore

\(^b\) Department of Mathematics, Middle East Technical University, İnönü Bulvarı, 06531 Ankara, Turkey

Abstract

We construct families of digital \((t, m, s)\)-nets over \(\mathbb{F}_4\) improving the best known parameters of \((t, m, s)\)-nets. We also improve the bound of Niederreiter and Xing in the asymptotic theory of digital \((t, m, s)\)-nets.

\textit{Keywords:} \((t, m, s)\)-Net; Digital net; Finite field; Linear code

1. Introduction

The theory of \((t, m, s)\)-nets provides powerful methods for the construction of low-discrepancy point sets. We refer to the monographs [15, Chapter 4], [17, Chapter 8] and the recent survey article [16] for the general background.

A special but very important class of nets are digital nets [11], [17, Chapter 8]. In this paper we restrict ourselves to the construction of digital nets over a finite field \(\mathbb{F}_q\). We obtain families of \((t, m, s)\)-nets over \(\mathbb{F}_4\) improving the best known parameters of \((t, m, s)\)-nets in [19]. We also improve the bound of Niederreiter and Xing [18, Theorem 2] (see also [16, Theorem 9.2]). Our results are constructive in many cases.

\(^*\) Corresponding author.

\textit{E-mail addresses:} lingsan@ntu.edu.sg (S. Ling), ozbudak@metu.edu.tr (F. Özbudak).
The paper is organized as follows. In Section 2 we recall some preliminaries. Our digital $(t, m, s)$-nets over $\mathbb{F}_4$ are explained in Section 3. We illustrate some improvements of Section 3 in Section 4 by comparing the parameters of our $(t, m, s)$-nets with the best known parameters of the $(t, m, s)$-nets as listed in the MinT database [19]. In Section 5 we improve the bound by Niederreiter and Xing in the asymptotic theory of digital $(t, m, s)$-nets.

2. Preliminaries

In this section we provide some basic facts and we fix the notation. The standard terminology on $(t, m, s)$-nets goes back to [14]. Let $I$ be the interval $[0, 1)$. Let $\mathbb{F}_q$ be a finite field. Let $m, s$ be positive integers and $C_1, \ldots, C_s$ be $m \times m$ matrices over $\mathbb{F}_q$. We recall the digital method of [17, Section 8.2] with the generating matrices $C_1, \ldots, C_s$. Let $\eta : \mathbb{F}_q \to \{0, 1, \ldots, q-1\}$ be a bijection and $\phi_{m} : \mathbb{F}_m^q \to I$ be defined as $(a_1, \ldots, a_m) \mapsto \sum_{j=1}^{m} \eta(a_j)q^{-j}$. We recall the convention in the area that a point set is used in the sense of combinatorics, that is, a set in which multiplicities of elements are allowed and taken into account. We consider the point set consisting of the points

\[
(\phi_{m}(nC_1), \ldots, \phi_{m}(nC_s)) \in I^s
\]

with the row vector $n$ running through $\mathbb{F}_m^q$.

For $1 \leq i \leq s$, let $c_{i}^{(1)}, \ldots, c_{i}^{(m)} \in \mathbb{F}_m^q$ be the column vectors of $C_i$. Let $\mathcal{C} = \{c_{i}^{(j)} : 1 \leq i \leq s, 1 \leq j \leq m\}$ be the system of vectors obtained from $C_1, \ldots, C_s$.

The following definition and theorem (see [17, Theorem 8.2.4]) are crucial.

**Definition 2.1.** Let $d$ be an integer with $0 \leq d \leq m$. The system $\mathcal{C}$ is a $(d, m, s)$-system over $\mathbb{F}_q$ if and only if for any nonnegative integers $d_1, \ldots, d_s$ with $\sum_{i=1}^{s} d_i = d$ the subsystem $\{c_{i}^{(j)} : 1 \leq i \leq s, 1 \leq j \leq d_i\}$ is linearly independent over $\mathbb{F}_q$ (the empty system is considered linearly independent).

Let $C$ be the $m \times ms$ matrix over $\mathbb{F}_q$ obtained from the matrices $C_1, \ldots, C_s$ by

\[
C = [C_1 \ C_2 \ \cdots \ C_s].
\]

The point set generated by $C$ refers to the point set in (2.1).

**Theorem 2.2.** The point set generated by $C$ is a digital $(t, m, s)$-net over $\mathbb{F}_q$ if and only if $\mathcal{C}$ is a $(d, m, s)$-system with $d = m - t$.

Let $C'$ be the $m \times ds$ submatrix of $C$ consisting of the first $d$ columns of $C_1, \ldots, C_s$ only. It follows from Theorem 2.2 that it is enough to consider $C'$ to prove that the digital net generated by $C$ is a $(t, m, s)$-net over $\mathbb{F}_q$ with $t$ not exceeding $m - d$. From now on, by a point set in $I^s$ constructed by a given $m \times ds$ matrix $M$ over $\mathbb{F}_q$ with given $s, 1 \leq d < m$ and $M = [M_1 \ M_2 \ \cdots \ M_s]$, we mean a point set obtained from (2.1) such that for each $1 \leq i \leq s$, an $m \times m$ generating matrix $C_i$ is obtained from the $m \times d$ matrix $M_i$ by appending $m - d$ arbitrarily chosen columns on the right-hand side.
Remark 2.3. In this paper we restrict ourselves only to digital \((t, m, s)\)-nets over a finite field. For the concept of \((t, m, s)\)-nets in general we refer to [16] and [17, Chapter 8]. It is known that there is a complete equivalence between \((t, m, s)\)-nets and certain ordered orthogonal arrays. We refer to [12, Section 5], [16, Section 6], and the references therein for the details of this equivalence and related results.

We fix the following notation throughout the paper. Let \(\omega \in \mathbb{F}_4\) be a fixed element such that \(\omega^2 + \omega + 1 = 0\). For a finite field \(F\), \(F^*\) denotes its multiplicative subgroup \(F \setminus \{0\}\). If \(E/F\) is an extension of finite fields, then \(\text{Tr}_{E/F}\) is the trace map from \(E\) onto \(F\). For a finite set \(S\), \(|S|\) denotes its cardinality.

3. Some \((t, m, s)\)-nets over \(\mathbb{F}_4\)

In this section we give our families of digital \((t, m, s)\)-nets over \(\mathbb{F}_4\). Each of them is presented in a subsection below. We use methods from [7], two families of \(\mathbb{F}_4\)-linear codes from [9] (see also [4], [1, Theorems 13.29 and 13.30]), and some results from [2].

3.1. Some \((t, m, s)\)-nets over \(\mathbb{F}_4\) with even \(m\)

Let \(m \geq 6\) be an even integer, \(f = m/2\) and \(q = 2^f\). We note that 3 divides \(q^2 - 1\) and we put \(s = (q^2 - 1)/3\). Let \(Z\) be a complete set of representatives of \(\mathbb{F}_q^*\)-cosets of the quotient group \(\mathbb{F}_q^*/\mathbb{F}_4^*\) and hence we have \(|Z| = s\). This implies that if \(a, b \in Z\) and \(a \neq b\), then \(a/b \not\in \mathbb{F}_4\). Note that \(Z\) can be chosen as the multiplicative subgroup of \(\mathbb{F}_q^*\) with \(|Z| = s\) if and only if \(f \equiv 1\) or 2 mod 3. We enumerate the elements of \(Z\) so that \(Z = \{z_1, z_2, \ldots, z_s\}\).

In Proposition 3.3 we prove that for each \(f \geq 3\) there exists \(\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_4\) such that

\[
\text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}\left(\frac{1}{\alpha}\right) = \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}\left(\frac{1}{\omega^2 + \omega\alpha}\right) = \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}\left(\frac{1}{\omega + \omega^2\alpha}\right) = 1. \tag{3.1}
\]

Moreover in Example 3.2 we will determine such \(\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_4\) satisfying (3.1) explicitly for \(3 \leq f \leq 8\).

Assume that we choose \(\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_4\) satisfying (3.1). Let \(T(\alpha)\) be the subset of \(\mathbb{F}_{q^2}\), depending on \(\alpha\), defined as

\[
T(\alpha) = \left\{ \frac{1}{u_1^2 + u_2^2 + \alpha^2} + u_1 + u_2\alpha : u_1, u_2 \in \mathbb{F}_4 \right\}. \tag{3.2}
\]

As \(f \geq 3\), we have \(|T(\alpha)| \leq 16 < q^2 - 1\) and hence we can choose \(\beta \in \mathbb{F}_{q^2} \setminus T(\alpha)\). For \(1 \leq i \leq s\), let \(M_i\) be the \(2 \times 4\) matrix over \(\mathbb{F}_{q^2}\) given by

\[
M_i = \begin{bmatrix}
\frac{z_i}{1/z_i^2} & \frac{z_i}{\alpha/z_i} & \frac{\alpha z_i^2}{\beta/z_i^2} & \frac{z_i + 1}{1/z_i^2 + 1}
\end{bmatrix},
\]
where $z_{s+1} = z_1$. Let $\Phi : \mathbb{F}_{q^2} \to \mathbb{F}_4^f$ be an $\mathbb{F}_4$-linear isomorphism. For $1 \leq i \leq s$, using $M_i$, we define the $m \times 4$ matrices $M_i$ over $\mathbb{F}_4$ as

$$M_i = \begin{bmatrix} \Phi(z_i) & \Phi(1/z_i^2) & \Phi(\alpha z_i) & \Phi(z_i+1) \\ \Phi(1/z_i^2) & \Phi(\alpha/z_i^2) & \Phi(\beta/z_i^2) & \Phi(1/z_i^2+1) \end{bmatrix}. \tag{3.3}$$

Finally let $M$ be the $m \times (4s)$ matrix over $\mathbb{F}_4$ defined by

$$M = [M_1 \ M_2 \ldots \ M_s]. \tag{3.4}$$

**Theorem 3.1.** Let $f \geq 3$ be an integer and $s = (2^{2f} - 1)/3$. Each point set in $I^s$ constructed by the matrix $M$ in (3.4) is a digital $(t, m, s)$-net over $\mathbb{F}_4$ with

$$t = m - 4, \quad m = 2f, \quad s = \frac{2^{2f} - 1}{3}.$$

Moreover such a digital $(t, m, s)$-net is as constructive as the constructiveness of $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_4$ satisfying (3.1).

**Proof.** For a positive integer $d$, let a partition of $d$ into positive integers $d_1, \ldots, d_{\ell}$ (so that $d = d_1 + \cdots + d_{\ell}$) be denoted as type $(d_1 + \cdots + d_{\ell})$ (cf. [7]). Using Theorem 2.2, it is sufficient to prove that for each positive integer $1 \leq d \leq 4$ and each type $(d_1 + \cdots + d_{\ell})$ partition of $d$, the corresponding systems of $d$ columns of $M$ are linearly independent over $\mathbb{F}_4$. In Definition 2.1, the summands of $d$ are considered to be nonnegative integers and there are $s$ such summands. Then each summation corresponds to a unique system consisting of $d$ columns of $M$. Here the summands of $d$ are positive integers and hence the number $\ell$ of summands is less than or equal to $d$. There may be more than one system corresponding to a given partition of $d$ since we have a choice of $\ell$ submatrices among $s$ matrices $M_1, \ldots, M_s$ of $M$. We note that as the corresponding point set is considered in the sense of combinatorics, i.e., multiplicities of its elements are taken into account (see Section 2), there is no need to show that the rank of $M$ is $m$, although this is the case, which follows from the rank of the matrix $H$ introduced below.

Let $H$ be the $m \times s$ matrix over $\mathbb{F}_4$ consisting of the first columns of the matrices $M_i$ for $1 \leq i \leq s$, which are defined in (3.3). It is known that $H$ is a parity check matrix of a linear $[s, s - m, 5]$-code over $\mathbb{F}_4$ [9] (see also [4], [1, Theorem 13.30]). Hence for each of the types $(1)$, $(1 + 1)$, $(1 + 1 + 1)$, and $(1 + 1 + 1 + 1)$, any corresponding system of columns of $M$ is linearly independent over $\mathbb{F}_4$.

It remains to consider the types $(2)$, $(3)$, $(2 + 1)$, $(4)$, $(3 + 1)$, $(2 + 2)$ and $(2 + 1 + 1)$. First we prove an observation which we will use later in the proof.

For $y \in \mathbb{F}_{q^2}^*$, we note that there exists $y \in \mathbb{F}_{q^2}^*$ with $y + 1/y = \gamma$ if and only if

$$\text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(1/y) = 0.$$

Indeed we have

$$y + 1/y = \gamma \iff y^2 + \gamma y = 1 \iff (y/\gamma)^2 + (y/\gamma) = 1/\gamma^2. \tag{3.5}$$
Using Hilbert’s Theorem 90 (cf. [13, Theorem 2.25]), for any \( x \in \mathbb{F}_{q^2} \) we have
\[
x^2 + x = 1/\gamma^2 \iff \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(1/\gamma^2) = \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(1/\gamma) = 0.
\] (3.6)

Combining (3.5) and (3.6) we get that there exists \( y \in \mathbb{F}_{q^2}^* \) with \( y + 1/y = \gamma \) if and only if \( \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(1/\gamma) = 0 \). Hence from (3.1) we obtain that for any \( y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_4 \) we have the following inequalities:
\[
y + 1/y \neq \alpha, \quad y + 1/y \neq \omega^2 + \alpha \omega, \quad \text{and} \quad y + 1/y \neq \omega + \alpha \omega^2.
\] (3.7)

In the following, for each of the remaining types mentioned above, we first assume that there exists a corresponding linearly dependent system of columns of \( M \) over \( \mathbb{F}_4 \), and then we prove this assumption gives a contradiction.

**Type (2).** We have \( a \in \mathbb{Z} \) and \( u_1, u_2 \in \mathbb{F}_4 \) with
\[
(u_1 + u_2)a = 0,
\]
\[
(u_1 + \alpha u_2)/a^2 = 0,
\]
and \( u_2 \neq 0 \). Indeed if \( u_2 = 0 \), then we are in the case of type (1). Moreover we can further assume that \( u_2 = 1 \) and \( u_1 \in \mathbb{F}_4 \) without loss of generality. (From now on throughout the paper, we will directly assume similar simplifications in the analysis of the possible types in the proofs, which hold without loss of generality.) Then \( u_1 + \alpha = 0 \), which is a contradiction as \( \alpha \notin \mathbb{F}_4 \).

**Type (3).** We have \( a \in \mathbb{Z} \) and \( u_1, u_2 \in \mathbb{F}_4 \) with
\[
(u_1 + u_2 + \alpha)a = 0,
\]
\[
(u_1 + \alpha u_2 + \beta)/a^2 = 0.
\]
Then \( u_1 + u_2 + \alpha = 0 \) gives a contradiction.

**Type (2+1).** We have distinct \( a, b \in \mathbb{Z} \) and \( u_1, u_2 \in \mathbb{F}_4 \) with
\[
(u_1 + 1)a = u_2 b,
\]
\[
(u_1 + \alpha)/a^2 = u_2/b^2,
\] (3.8)
and \( u_2 \neq 0 \). Taking the square of the first equation of (3.8) and multiplying it with the second equation of (3.8) we obtain
\[
(u_1 + 1)^2(u_1 + \alpha) = u_2^3 = 1,
\]
which is a contradiction as \( \alpha \notin \mathbb{F}_4 \).

**Type (2+1+1).** We have distinct \( a, b, c \in \mathbb{Z} \) and \( u_1, u_2, u_3 \in \mathbb{F}_4 \) with
\[
(u_1 + 1)a = u_2 b + u_3 c,
\]
\[
(u_1 + \alpha)/a^2 = u_2/b^2 + u_3/c^2,
\]
and $u_2 \neq 0$, $u_3 \neq 0$. Then we get

$$(u_1 + 1)^2(u_1 + \alpha) = (u_2^2b^2 + u_3^2c^2)(u_2/b^2 + u_3/c^2).$$

(3.9)

Let $u = u_2^2u_3 \in \mathbb{F}_4^*$, $x = (b/c)^2$ and $y = ux$. As $b, c \in Z$ and $b \neq c$, we have $b/c \not\in \mathbb{F}_4$ and hence $y \in \mathbb{F}_4^2 \setminus \mathbb{F}_4$. Using $u_2^2 = u_3^3 = 1$ and (3.9) we obtain that

$$y + 1/y = (u_1 + 1)^2(u_1 + \alpha).$$

If $u_1 = 0$, then $y + 1/y = \alpha$, which is a contradiction to (3.7).

If $u_1 = 1$, then $y + 1/y = 0$ and hence $y = 1 \in \mathbb{F}_4$, which is a contradiction.

Finally if $u_1 = \omega^2$, then $y + 1/y = (\omega^2 + 1)^2(\omega^2 + \alpha) = \omega + \omega^2\alpha$, which is again a contradiction to (3.7).

**Type (2+2).** We have distinct $a, b \in Z$ and $u_1, u_2, u_3 \in \mathbb{F}_4$ with

$$(u_1 + 1)a = (u_2 + u_3)b,$$

$$(u_1 + \alpha)a^2 = (u_2 + au_3)/b^2,$$

(3.10)

and $u_3 \neq 0$. If $u_1 = 1$, then $u_2 = u_3$ and hence we have

$$(1 + \alpha)/a^2 = u_3(1 + \alpha)/b^2,$$

which implies that $(b/a)^2 = u_3 \in \mathbb{F}_4$, and hence $b/a \in \mathbb{F}_4$, which is a contradiction. Note that $1 + \alpha \neq 0$ as $\alpha \neq \mathbb{F}_4$.

If $u_1 \neq 1$, then $u_2 \neq u_3$ and using (3.10) we obtain

$$(u_1 + 1)^2(u_1 + \alpha) = (u_2 + u_3)^2(u_2 + au_3).$$

Then $u_1^3 + u_1 + \alpha u_1^2 + \alpha = u_2^3 + u_2u_3 + \alpha u_3u_2 + \alpha u_3^2$ and using $u_3^3 = 1$ we get

$$\alpha(u_2^2u_3 + u_1^2) = u_2^3 + u_2u_3^2 + u_1^3 + u_1.$$
which implies that $\beta \in T(\alpha)$, where $T(\alpha)$ is the set given in (3.2). However this is a contradiction to the definition of $\beta$.

**Type (4).** By definition of the matrix $M$, the proof of the case of type $(3+1)$ also gives a proof of type (4). \hfill \Box

In the next example we construct $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_4$ satisfying (3.1) explicitly for $3 \leq f \leq 8$.

**Example 3.2.** We note that if $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_4$ satisfies the conditions in (3.1), then $\alpha^2$ also satisfies the conditions in (3.1). Therefore if $P_\alpha(x) \in \mathbb{F}_2[x]$ is the minimal polynomial of $\alpha$ over $\mathbb{F}_2$, then any root of $P_\alpha(x)$ satisfies the conditions in (3.1). In Table 1, for each $3 \leq f \leq 8$, we explicitly determine a polynomial $P_\alpha(x) \in \mathbb{F}_2[x]$ such that $P_\alpha(x)$ has no root in $\mathbb{F}_4$ and all of the roots of $P_\alpha(x)$ satisfy the conditions in (3.1).

In the next proposition we use some results from [2].

**Proposition 3.3.** Let $f \geq 3$ be an integer and $q = 2^f$. There exists $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_4$ satisfying the condition (3.1).

**Proof.** Using Example 3.2, it is enough to prove the proposition for $f \geq 9$. We will prove the existence of a primitive element $\alpha \in \mathbb{F}_{q^2}$ satisfying (3.1) for $f \geq 9$. Let $g_1(x), g_2(x), g_3(x)$ be the rational functions in $\mathbb{F}_{q^2}(x)$ given by

$$g_1(x) = \frac{1}{x}, \quad g_2(x) = \frac{1}{\omega^2 + \omega x}, \quad g_3(x) = \frac{1}{\omega + \omega^2 x}.$$ 

Recall that $\{g_1(x), g_2(x), g_3(x)\}$ is strongly linearly independent over $\mathbb{F}_2$ (cf. [2]) if the existence of $a_1, a_2, a_3 \in \mathbb{F}_2, g(x) \in \mathbb{F}_{q^2}(x)$ and $\xi \in \mathbb{F}_{q^2}$ satisfying

$$a_1 g_1(x) + a_2 g_2(x) + a_3 g_3(x) = g(x)^2 - g(x) + \xi \quad (3.11)$$

implies that $a_1 = a_2 = a_3 = 0$. Let $P_1$ be the pole of $\mathbb{F}_{q^2}(x)$ corresponding to the zero of $x$ and let $v_{P_1}$ be the normalized discrete valuation corresponding to $P_1$ (cf. [17, Section 1.1]). If (3.11) holds with $a_1 \neq 0$, then $v_{P_1}(g_1(x)) = v_{P_1}(a_1 g_1(x)) = -1$, $v_{P_1}(a_2 g_2(x)) \geq 0$, $v_{P_1}(a_3 g_3(x)) \geq 0$ and hence

$$v_{P_1}(g(x)^2 - g(x) + \xi) = v_{P_1}(a_1 g_1(x) + a_2 g_2(x) + a_3 g_3(x)) = -1. \quad (3.12)$$

### Table 1

Construction of $\alpha$ satisfying the conditions in (3.1)

<table>
<thead>
<tr>
<th>$f$</th>
<th>$P_\alpha(x) \in \mathbb{F}_2[x]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>$x^6 + x^4 + x^3 + x + 1$</td>
</tr>
<tr>
<td>4</td>
<td>$x^8 + x^7 + x^6 + x^4 + x^2 + x + 1$</td>
</tr>
<tr>
<td>5</td>
<td>$x^{10} + x^9 + x^8 + x^7 + x^2 + x + 1$</td>
</tr>
<tr>
<td>6</td>
<td>$x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$</td>
</tr>
<tr>
<td>7</td>
<td>$x^{14} + x^{11} + x^9 + x^7 + x^3 + x + 1$</td>
</tr>
<tr>
<td>8</td>
<td>$x^{16} + x^{15} + x^{14} + x^{11} + x^8 + x^7 + x^4 + x + 1$</td>
</tr>
</tbody>
</table>
Then \( v_{P_1}(g(x)) < 0 \). Indeed if \( v_{P_1}(g(x)) \geq 0 \), then \( v_{P_1}(g(x)^2 - g(x) + \xi) \geq 0 \), which contradicts (3.12). As \( v_{P_1}(g(x)) < 0 \) we have \( v_{P_1}(g(x)^2 - g(x) + \xi) = 2v_{P_1}(g(x)) \) and 2 divides \( v_{P_1}(g(x)^2 - g(x) + \xi) \). This is a contradiction to (3.12). For \( i = 2, 3 \), if (3.11) holds with \( a_i \neq 0 \), then similarly using the valuation at the place corresponding to the zero of the denominator of \( g_i(x) \) we obtain a contradiction.

Under the notation of [2, Theorem 1.1], we have \( r = 3, m = 1 \) and \( l = 1 \). Then by [2, Theorem 1.1] if

\[
2.f > 4(3 + \log_2(9.8r)) = 31.51 \ldots,
\]

then there exists a primitive \( \alpha \in \mathbb{F}_{q^2} \) satisfying (3.1).

We will prove the remaining cases \( 9 \leq f \leq 15 \) using [2, Theorem 3.1]. Under the notation of [2, Theorem 3.1] we have \( D = 20, \delta_2f = 0, E = 14 \). For \( 11 \leq f \leq 15 \), taking \( s = 1 \) and noting that the numbers of distinct prime factors of \( 2^{22} - 1, 2^{24} - 1, 2^{26} - 1, 2^{28} - 1 \) and \( 2^{30} - 1 \) are 4, 6, 3, 6, and 6, respectively, we obtain the existence of a primitive \( \alpha \in \mathbb{F}_{q^2} \) satisfying (3.1) by observing that [2, Condition (3.5)] holds.

For \( f = 9 \), we take \( l = 1 \) and hence we have \( s = 4 \) in [2, Theorem 3.1]. Therefore \( \sigma = 1 - (\frac{1}{3} + \frac{1}{5} + \frac{1}{9} + \frac{1}{17}) \) and [2, condition (3.5)] holds. Finally for \( f = 1 \) and \( s = 5 \) in [2, Theorem 3.1]. Therefore \( \sigma = 1 - (\frac{1}{3} + \frac{1}{5} + \frac{1}{11} + \frac{1}{17} + \frac{1}{47}) \) and [2, condition (3.5)] holds again. This completes the proof. \( \square \)

### 3.2. Some \((t, m, s)\)-nets over \( \mathbb{F}_4 \) with odd \( m \)

Let \( m \geq 7 \) be an odd integer, \( f = m \) and \( q = 2^f \). We note that 3 divides \( q + 1 \) and we put \( s = (q + 1)/3 \). Let \( W \) be the subgroup of \( \mathbb{F}_{q^2}^* \) with \( |W| = q + 1 \). We have \( W \cap \mathbb{F}_q = \{1\} \). Let \( Z \) be a complete set of representatives of \( \mathbb{F}_{q^2}^* / \mathbb{F}_q^* \)-cosets of the quotient group \( W/\mathbb{F}_q^* \) and hence we have \( |Z| = s \). This implies that if \( a, b \in Z \) and \( a \neq b \), then \( a/b \notin \mathbb{F}_4 \). Note that \( Z \) can be chosen as the multiplicative subgroup of \( \mathbb{F}_{q^2}^* \) with \( |Z| = s \) if and only if \( f \equiv 1 \) or \( 5 \mod 6 \) (cf. Section 3.1). We enumerate the elements of \( Z \) such that \( Z = \{z_1, z_2, \ldots, z_s\} \).

Let \( S \) be the subset of \( \mathbb{F}_{q^2} \) defined by

\[
S = \left\{ y + \frac{1}{y} : y \in W \setminus \{1\} \right\}. \tag{3.13}\]

Note that \( 1 = \omega + \omega^2 \in S \) as \( \mathbb{F}_4^* \subseteq W \). For \( y_1, y_2 \in W \setminus \mathbb{F}_2 \) we have

\[
y_1 + \frac{1}{y_1} = y_2 + \frac{1}{y_2} \iff y_1 = y_2 \quad \text{or} \quad y_1 = \frac{1}{y_2}.
\]

Moreover there is no \( y \in W \setminus \mathbb{F}_2 \) with \( y = 1/y \). Hence \( |S| = q/2 \). Our construction in this subsection depends on the following assumption.

**Assumption 3.4.** We assume that there exists \( \alpha \in \mathbb{F}_{q^2} \) such that

\[
\alpha^{q-1} \notin \mathbb{F}_4, \quad (u + \alpha)^{q+1} \notin S \quad \text{for each} \ u \in \mathbb{F}_4, \quad \text{and}
\]

\[
(1 + v/\alpha)^{q+1} \neq 1 \quad \text{for each} \ v \in \mathbb{F}_4^* \tag{3.14}
\]
In particular we note that $\alpha \notin F_4$, since otherwise $\alpha^{q-1} \in F_4$.

We will show that Assumption 3.4 is valid at least for $f \in \{7, 9, 11, 13, 15, 17, 19\}$ by determining such $\alpha$ satisfying the assumption explicitly in Example 3.6. We note that Assumption 3.4 would be wrong if $f$ were in $\{3, 5\}$.

Assume that we choose $\alpha \in F_{q^2}$ satisfying Assumption 3.4. There are exactly $q + 1$ elements $\gamma \in F_{q^2}$ with $\gamma^{q+1} = 1$. Hence there are at most $16(q + 1)$ elements $\gamma \in F_{q^2}$ such that for some $u_1, u_2 \in F_4$ we have $(u_1 + u_2\alpha + \gamma)^{q+1} = 1$. Moreover there are exactly 16 elements $\gamma \in F_{q^2}$ such that for some $u_1, u_2 \in F_4$ we have $u_1 + u_2\alpha + \gamma = 0$. As $f \geq 7$ we have $q^2 > (16(q + 1) + 16)$. Therefore there exists $\beta \in F_{q^2}$ such that

$$(u_1 + u_2\alpha + \gamma)^{q+1} \neq 1 \quad \text{and} \quad u_1 + u_2\alpha + \beta \neq 0, \quad \text{for all } u_1, u_2 \in F_4. \tag{3.15}$$

It is not difficult to determine such $\beta$. In Example 3.6, we will also determine such $\beta$ explicitly for $f \in \{7, 9, 11, 13, 15, 17, 19\}$.

For $1 \leq i \leq s$, let $M_i$ be the $1 \times 4$ matrix over $F_{q^2}$ given by

$$M_i = [z_i \alpha z_i \beta z_i z_{i+1}],$$

where $z_{s+1} = z_1$. Let $\Phi : F_{q^2} \to F_4^f$ be an $F_4$-linear isomorphism. For $1 \leq i \leq s$, using $M_i$, we define the $m \times 4$ matrix $M_i$ over $F_4$ as

$$M_i = \begin{bmatrix} \Phi(z_i) & \Phi(\alpha z_i) & \Phi(\beta z_i) & \Phi(z_{i+1}) \end{bmatrix}. \tag{3.16}$$

Finally let $M$ be the $m \times (4s)$ matrix over $F_4$ defined by

$$M = \begin{bmatrix} M_1 & M_2 & \ldots & M_s \end{bmatrix}. \tag{3.17}$$

**Theorem 3.5.** Let $f \geq 7$ be an odd integer, $s = (2f + 1)/3$ and assume that Assumption 3.4 holds. Each point set in $I^s$ constructed by the matrix $M$ in (3.17) is a digital $(t, m, s)$-net over $F_4$ with

$$t = m - 4, \quad m = f, \quad s = \frac{2f + 1}{3}.$$

Moreover such a digital $(t, m, s)$-net is as constructive as the constructiveness of the elements $\alpha, \beta \in F_{q^2}$ satisfying (3.14) and (3.15), respectively.

**Proof.** Let $H$ be the $m \times s$ matrix over $F_4$ consisting of the first columns of the matrices $M_i$ for $1 \leq i \leq s$, which are defined in (3.17). It is known that $H$ is a parity check matrix of a linear $[s, s - m, 5]$-code over $F_4$ [9] (see also [4], [1, Theorem 13.29]). Therefore, as in the proof of Theorem 3.1, it is enough to consider the following types.

**Type (2).** We have $a \in \mathbb{Z}$ and $u_1 \in F_4$ with

$$(u_1 + \alpha)a = 0.$$ 

Then $\alpha \in F_4$, which is a contradiction.
Type (3). We have \( a \in \mathbb{Z} \) and \( u_1, u_2 \in \mathbb{F}_4 \) with

\[(u_1 + u_2 \alpha + \beta)a = 0.\]

Then \( u_1 + u_2 \alpha + \beta = 0 \), which is a contradiction to (3.15).

Type (2+1). We have distinct \( a, b \in \mathbb{Z} \) and \( u_1, u_2 \in \mathbb{F}_4 \) with

\[(u_1 + \alpha)a = u_2b,\]

and \( u_2 \neq 0 \). Taking \((q + 1)\)th powers we obtain \((u_1 + \alpha)^{q+1} = 1\), which is a contradiction to Assumption 3.4 as \( 1 \in S \).

Type (2+1+1). We have distinct \( a, b, c \in \mathbb{Z} \) and \( u_1, u_2, u_3 \in \mathbb{F}_4 \) with

\[(u_1 + \alpha)a = u_2b + u_3c,\]

\( u_2 \neq 0 \), and \( u_3 \neq 0 \). Taking \((q + 1)\)th powers we obtain

\[(u_1 + \alpha)^{q+1} = (u_2b + u_3c)(u_2^2/b + u_3^2/c).\]

Let \( u = u_2u_3^2 \in \mathbb{F}_4^* \) and \( y = ub/c \in W \setminus \mathbb{F}_2 \). Then we obtain

\[(u_1 + \alpha)^{q+1} = y + \frac{1}{y} \in S,\]

which is a contradiction to Assumption 3.4.

Type (2+2). We have distinct \( a, b \in \mathbb{Z} \) and \( u_1, u_2, u_3 \in \mathbb{F}_4 \) with

\[(u_1 + \alpha)a = (u_2 + \alpha u_3)b, \quad (3.18)\]

and \( u_3 \neq 0 \). Let \( v = \alpha^{q-1} \). By Assumption 3.4 we have \( v \notin \mathbb{F}_4 \) and by definition we have \( \alpha^q = v \alpha \). Taking \((q + 1)\)th powers of (3.18) we obtain \((u_1^2 + v \alpha)(u_1 + \alpha) = (u_2^2 + u_3^2v \alpha)(u_2 + u_3\alpha)\) and, using \( u_3^3 = 1 \), we get

\[u_1^3 + \alpha(u_1^2 + vu_1) = u_2^3 + \alpha(u_2^2u_3 + vu_2u_3^2). \quad (3.19)\]

Assume first that \( u_1^2 + vu_1 \neq u_2^2u_3 + vu_2u_3^2 \). Then by (3.19) we obtain \( u_1 = u_2 \neq u_3 \), since \( \alpha \neq 0 \). This implies that either \( u_1 = 0 \) and \( u_2 \neq 0 \), or \( u_1 \neq 0 \) and \( u_2 = 0 \). If \( u_1 = 0 \) and \( u_2 \neq 0 \), then by (3.18) we have

\[\frac{a}{b} = u_3 \left( \frac{u + \alpha}{\alpha} \right).\]
where \( u = u_2/u_3 \in \mathbb{F}_4^* \). Taking \((q + 1)\)th powers we obtain \((1 + u/\alpha)^{q+1} = 1\), which is a contradiction to Assumption 3.4. If \( u_1 \neq 0 \) and \( u_2 = 0 \), then by (3.18) we have
\[
\frac{b}{a} = \frac{1}{u_3} \left( \frac{u_1 + \alpha}{\alpha} \right).
\]
Similarly taking \((q + 1)\)th powers contradicts Assumption 3.4.

Therefore we have \( u_1^2 + vu_1 = u_2^2u_3 + vu_2u_3^2 \). As \( v \notin \mathbb{F}_4 \), this implies that \( u_1^2 = u_2^2u_3 \) and \( u_1 = u_2u_3^2 \). Then by (3.18) we obtain
\[
\frac{b}{a} = \frac{u_1 + \alpha}{u_2 + u_3} = \frac{u_2u_3^2 + \alpha}{u_2 + u_3} = \frac{u_3(u_2 + \alpha u_3)}{u_2 + u_3} = u_3 \in \mathbb{F}_4,
\]
which is a contradiction. Note that \( u_2 + \alpha u_3 \neq 0 \) as \( \alpha \notin \mathbb{F}_4 \) and \( u_3 \neq 0 \).

**Type (3+1).** We have distinct \( a, b \in \mathbb{Z} \) and \( u_1, u_2, u_3 \in \mathbb{F}_4 \) with
\[
(u_1 + \alpha u_2 + \beta)a = u_3b,
\]
and \( u_3 \neq 0 \). Then taking \((q + 1)\)th powers we obtain that
\[
(u_1 + \alpha u_2 + \beta)^{q+1} = 1,
\]
which is a contradiction to (3.15).

**Type (4).** By definition of the matrix \( \mathcal{M} \), the proof of the case of type \((3 + 1)\) also gives a proof of type (4). \(\Box\)

In the next example, we first construct \( \alpha \in \mathbb{F}_{q^2}^* \) satisfying (3.14), and then using such an \( \alpha \) we construct \( \beta \in \mathbb{F}_{q^2}^* \) satisfying (3.15), both for \( f \in \{7, 9, 11, 13, 15, 17, 19\} \) explicitly.

**Example 3.6.** Recall that \( S \) defined in (3.13) is a subset of \( \mathbb{F}_{q^2} \). We first assert that \( \gamma \in S \iff \gamma^2 \in S \). Indeed let \( \gamma = y + 1/y \) with \( y \in W \setminus \mathbb{F}_2 \). We have \( y^2 \in W \setminus \mathbb{F}_2 \) and \( \gamma^2 = y^2 + 1/y^2 \), which proves our assertion in one direction. The other direction follows from the fact that the map \( x \mapsto x^2 \) is a field automorphism of \( \mathbb{F}_{q^2} \). Thus there exists \( u_1 \in \mathbb{F}_4 \) such that \((u_1 + \alpha)^{q+1} \in S \) if and only if there exists \( u_2 \in \mathbb{F}_4 \) such that \((u_2 + \alpha^2)^{q+1} \in S \). Similarly \( \alpha^{q-1} \in \mathbb{F}_4 \iff \alpha^{2(q-1)} \in \mathbb{F}_4 \). Also there exists \( v_1 \in \mathbb{F}_4^* \) such that \((1 + v_1/\alpha)^{q+1} = 1 \) if and only if there exists \( v_2 \in \mathbb{F}_4^* \) such that \((1 + v_2/\alpha^2)^{q+1} = 1 \). Hence in order to give an element \( \alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_4 \) satisfying Assumption 3.4, it is enough to give its minimal polynomial \( P_\alpha[x] \in \mathbb{F}_2[x] \) since if \( \alpha \) satisfies Assumption 3.4, then each of the roots of \( P_\alpha[x] \) satisfies Assumption 3.4. In Table 2 we determine such a minimal polynomial \( P_\alpha[x] \in \mathbb{F}_2[x] \) for each \( m \in \{7, 9, 11, 13, 15, 17, 19\} \). Moreover in Table 2, again for each \( m \in \{7, 9, 11, 13, 15, 17, 19\} \), we also give the minimal polynomial \( P_\beta[x] \in \mathbb{F}_2[x] \) of an element \( \beta \in \mathbb{F}_{q^2} \) satisfying (3.15) for a root \( \alpha' \) of the corresponding minimal polynomial \( P_\alpha[x] \) of the table.
3.3. Another family of \((t,m,s)\)-nets over \(\mathbb{F}_4\) with even \(m\)

Let \(m \geq 4\) be an even integer, \(f = m - 1\) and \(q = 2^f\). Note that \(f \geq 3\) is an odd integer and we put \(s = (q + 1)/3\). Let \(Z\) be the subset of \(\mathbb{F}_q^*\) with \(|Z| = s\) chosen as in Section 3.2. Again, we enumerate the elements of \(Z\) so that \(Z = \{z_1, z_2, \ldots, z_s\}\).

Let \(g\) be a generator of \(\mathbb{F}_q^*\), and we define \(\alpha = g^{q-1}\) and \(\beta = g^{q+1}\). For \(1 \leq i \leq s\), let \(M_i\) be the \(2 \times 4\) matrix over \(\mathbb{F}_q\) given by

\[
M_i = \begin{bmatrix} z_i & \alpha z_i & \beta z_i & z_{i+1} \\ 0 & 1 & 0 & 0 \end{bmatrix},
\]

where \(z_{s+1} = z_1\). Let \(\Phi : \mathbb{F}_q^2 \to \mathbb{F}_4^{(m-1)}\) be an \(\mathbb{F}_4\)-linear isomorphism. For \(1 \leq i \leq s\), using \(M_i\), we define the \(m \times 4\) matrix \(M_i\) over \(\mathbb{F}_4\) as

\[
M_i = \begin{bmatrix} \Phi(z_i) & \Phi(\alpha z_i) & \Phi(\beta z_i) & \Phi(z_{i+1}) \\ 0 & 1 & 0 & 0 \end{bmatrix}.
\]  

(3.20)

Finally let \(M\) be the \(m \times (4s)\) matrix over \(\mathbb{F}_4\) defined by

\[
M = [ M_1 \quad M_2 \quad \ldots \quad M_s ].
\]  

(3.21)
Theorem 3.7. Let \( f \geq 3 \) be an odd integer and \( s = (2^f + 1)/3 \). Each point set in \( I^s \) constructed by the matrix \( M \) in (3.21) is a constructive digital \((t, m, s)\)-net over \( \mathbb{F}_4 \) with

\[
t = m - 4, \quad m = f + 1, \quad s = \frac{2^f + 1}{3}.
\]

Proof. First note that \( \beta \in \mathbb{F}_q \setminus \mathbb{F}_4 \). Moreover \( \{1, \alpha, \alpha^q\} \) is linearly independent over \( \mathbb{F}_4 \). Indeed, assume that there exist \( u_1, u_2, u_3 \in \mathbb{F}_4 \), not all zero, such that

\[
(u_1 + u_2 \alpha + u_3 \alpha^q) = 0.
\]

Since \( \alpha^q = (g^{q - 1})^q = g^{q^2 - q} = g^{1 - q} = \frac{1}{g^{q-1}} = \frac{1}{\alpha} \), we have \( u_1 + u_2 \alpha + u_3 \frac{1}{\alpha} = 0 \) and hence

\[
u_2 \alpha^2 + u_1 \alpha + u_3 = 0.
\]

Therefore \( \alpha \) satisfies a quadratic equation over \( \mathbb{F}_4 \) and hence \( \alpha \in \mathbb{F}_4^2 \). However \( \mathbb{F}_4^2 \cap \mathbb{F}_q^2 = \mathbb{F}_4 \) and \( \alpha \notin \mathbb{F}_4 \), which gives a contradiction.

Let \( H \) be the \( m \times s \) matrix over \( \mathbb{F}_4 \) consisting of the first columns of the matrices \( M_i \) for \( 1 \leq i \leq s \), which are defined in (3.20). Let \( H_1 \) be the \((m - 1) \times s\) submatrix of \( H \) consisting of the first \( m - 1 \) rows of \( H \). As in the proof of Theorem 3.5, \( H_1 \) is a parity check matrix of a linear \([s, s - m + 1, 5]\)-code over \( \mathbb{F}_4 \) [9] (see also [4], [1, Theorem 13.29]). Hence, again, it is enough to consider the following types.

Type (2). We have \( a \in \mathbb{Z} \) and \( u_1 \in \mathbb{F}_4 \) with

\[
(u_1 + \alpha)a = 0,
\]

\[
1 = 0,
\]

which is a contradiction.

Type (3). We have \( a \in \mathbb{Z} \) and \( u_1, u_2 \in \mathbb{F}_4 \) with

\[
(u_1 + \alpha u_2 + \beta)a = 0,
\]

\[
u_2 = 0.
\]

Then \( \beta = u_1 \in \mathbb{F}_4 \), which is a contradiction.

Type (2+1). Similar to type (2).

Type (2+1+1). Similar to type (2).

Type (2+2). We have distinct \( a, b \in \mathbb{Z} \) and \( u_1, u_2, u_3 \in \mathbb{F}_4 \) with

\[
(u_1 + \alpha)a = (u_2 + \alpha u_3)b,
\]

\[
1 = u_3.
\]

(3.22)
Taking \((q + 1)\)th powers of the first equation in (3.22), and using \(u_3 = 1\) together with the fact \(a^{q+1} = b^{q+1} = 1\), we obtain that
\[
(u_1 + \alpha)(u_1^2 + \alpha^q) = (u_2 + \alpha)(u_2^2 + \alpha^q)
\]
and hence
\[
(u_1^3 + u_2^3) + (u_1^2 + u_2^2)\alpha + (u_1 + u_2)\alpha^q = 0.
\]
Recall that, in the beginning of the proof, we have shown that \(\{1, \alpha, \alpha^q\}\) is linearly independent over \(\mathbb{F}_4\). Hence \(u_1 = u_2\). Note that \(u_1 + \alpha \neq 0\) as \(\alpha \notin \mathbb{F}_4\). Using (3.22) we obtain that \(a = b\), which is a contradiction.

**Type (3+1).** We have distinct \(a, b \in \mathbb{Z}\) and \(u_1, u_2, u_3 \in \mathbb{F}_4\) with
\[
(u_1 + \alpha u_2 + \beta)a = u_3b,
\]
\[
u_2 = 0,
\]
and \(u_3 \neq 0\). Then we have
\[
(u_1 + \beta)a = u_3b.
\]
Taking \((q + 1)\)th powers and using the facts \(a^{q+1} = b^{q+1} = 1\), \(u_3^{q+1} = u_3^3 = 1\), \(\beta^q = \beta\), we obtain that
\[
(u_1 + \beta)(u_1^2 + \beta) = 1
\]
and hence
\[
u_1^3 + \beta(u_1^2 + u_1) + \beta^2 = 1.
\]
If \(u_1 = 0\), then \(\beta = 1\), which is a contradiction. If \(u_1 = 1\), then \(\beta = 0\), which is also a contradiction. If \(u_1 \in \mathbb{F}_4 \setminus \mathbb{F}_2\), then \(u_1^3 = 1\), \(u_1^2 + u_1 = 1\) and hence \(\beta^2 + \beta = 0\). This implies that \(\beta \in \mathbb{F}_2\), which is again a contradiction.

**Type (4).** By definition of the matrix \(\mathcal{M}\), the proof of the case of type \((3 + 1)\) also gives a proof of type \((4)\). \(\square\)

### 4. Comparisons

In this section we illustrate some of the improvements in Section 3 by comparing their parameters with the best known parameters of \((t, m, s)\)-nets in [19].

We observe that Theorem 3.1 (respectively Theorem 3.5) gives a family of digital \((t, m, s)\)-nets over \(\mathbb{F}_4\) for each even integer \(m \geq 6\) (respectively each odd integer \(m \geq 7\) provided Assumption 3.4 holds). In fact Theorem 3.1 (respectively Theorem 3.5) is also constructive at least for even integers \(6 \leq m \leq 16\) (respectively for odd integers \(7 \leq m \leq 19\)) since we explicitly
Table 3
Comparisons of Theorems 3.1 and 3.7 with the best known parameters in [19]

<table>
<thead>
<tr>
<th>$m$</th>
<th>Theorem 3.1</th>
<th>Theorem 3.7</th>
<th>[19] constructive and digital</th>
<th>[19] digital</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>21</td>
<td>11</td>
<td>19</td>
<td>19</td>
</tr>
<tr>
<td>8</td>
<td>85</td>
<td>43</td>
<td>85</td>
<td>85</td>
</tr>
<tr>
<td>10</td>
<td>341</td>
<td>171</td>
<td>341</td>
<td>341</td>
</tr>
<tr>
<td>12</td>
<td>1365</td>
<td>683</td>
<td>683</td>
<td>965</td>
</tr>
<tr>
<td>14</td>
<td>5461</td>
<td>2731</td>
<td>2730</td>
<td>3861</td>
</tr>
<tr>
<td>16</td>
<td>21845</td>
<td>10923</td>
<td>10922</td>
<td>15446</td>
</tr>
<tr>
<td>18</td>
<td>87381</td>
<td>43691</td>
<td>43690</td>
<td>61787</td>
</tr>
<tr>
<td>20</td>
<td>349525</td>
<td>174763</td>
<td>174762</td>
<td>247151</td>
</tr>
<tr>
<td>22</td>
<td>1398101</td>
<td>699051</td>
<td>699050</td>
<td>988606</td>
</tr>
<tr>
<td>24</td>
<td>5592405</td>
<td>2796203</td>
<td>2796202</td>
<td>3954427</td>
</tr>
</tbody>
</table>

Table 4
Comparison of Theorem 3.5 with the best known parameters in [19]

<table>
<thead>
<tr>
<th>$m$</th>
<th>Theorem 3.5</th>
<th>[19] constructive and digital</th>
<th>[19] digital</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>43</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>9</td>
<td>171</td>
<td>171</td>
<td>171</td>
</tr>
<tr>
<td>11</td>
<td>683</td>
<td>683</td>
<td>683</td>
</tr>
<tr>
<td>13</td>
<td>2731</td>
<td>1365</td>
<td>1930</td>
</tr>
<tr>
<td>15</td>
<td>10923</td>
<td>5461</td>
<td>7723</td>
</tr>
<tr>
<td>17</td>
<td>43691</td>
<td>21845</td>
<td>30893</td>
</tr>
<tr>
<td>19</td>
<td>174763</td>
<td>87381</td>
<td>123575</td>
</tr>
</tbody>
</table>

construct the corresponding $\alpha$ (respectively the corresponding $\alpha$ and $\beta$) in Example 3.2 (respectively Example 3.6). We observe that Theorems 3.1 and 3.5 give families of digital $(t,m,s)$-nets improving the corresponding best known parameters of digital $(t,m,s)$-nets in [19].

Theorem 3.7 gives a family of constructive and digital $(t,m,s)$-nets over $\mathbb{F}_4$ for each even integer $m \geq 4$. We observe that Theorem 3.7 improves the best known parameters of constructive and digital $(t,m,s)$-nets over $\mathbb{F}_4$ for even integers $m \geq 14$.

In Table 3, we compare the parameters of Theorems 3.1 and 3.7 with the corresponding best known parameters of digital and constructive, and digital $(t,m,s)$-nets in [19]. Similarly we compare Theorem 3.5 with [19] in Table 4. In these tables, for given values of $m$, the corresponding values of $s$ are tabulated. We observe that in Theorems 3.1 and 3.5, the differences between the improved values of $s$ and the best previously known values of $s$ in [19] are quite significant. For the ranges of $m$ in Tables 3 and 4, the corresponding $(t,m,s)$-nets in [19] with the best known parameters are all digital.

Remark 4.1. It is clear that Theorem 3.1 gives $(t,m,s)$-nets over $\mathbb{F}_4$ with much better parameters than those of Theorem 3.7. Moreover Theorem 3.7 improves the corresponding results in [19] only marginally. Comparing Theorems 3.1 and 3.7, the only point is that Theorem 3.7 could be seen more constructive compared to Theorem 3.1 since we need to choose $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_4$ satisfying (3.1) in Theorem 3.1. Otherwise the whole Section 3.3 could be ignored.
5. An improvement in the asymptotic

In this section we improve the bound of Niederreiter and Xing [18, Theorem 2] in the asymptotic theory of digital \((t, m, s)\)-nets for some parameters. We refer to [18] and [16, Section 9] for more information on the asymptotic theory of digital \((t, m, s)\)-nets. We use methods and results from [18,20], and some references in [20].

We first recall an important result of Niederreiter and Xing (cf. [18, Lemma 2]). For a prime power \(q\) and integers \(r \geq \alpha \geq 2\), let \(M_d(r, q)\) denote the largest value of \(n\) for which there exists a linear \([n, n - r, \alpha + 1]\)-code over \(\mathbb{F}_q\) (cf. [18, Definition 12]).

**Lemma 5.1 (Niederreiter–Xing).** For every prime power \(q\) and every integer \(\alpha \geq 2\), there exists a sequence of digital \((tr, tr + \alpha, sr)\)-nets constructed over \(\mathbb{F}_q\) with \(sr \to \infty\) as \(r \to \infty\) and

\[
\lim_{r \to \infty} \frac{tr}{log_q sr} = \liminf_{r \to \infty} \frac{r}{log_q M_d(r, q)}.
\]

Using BCH codes and Lemma 5.1, Niederreiter and Xing obtained the following result in [18, Theorem 2].

**Theorem 5.2 (Niederreiter–Xing).** Let \(d \geq 2\) be an integer and \(q\) be a prime power. There exists a sequence of digital \((tr, tr + d, sr)\)-nets over \(\mathbb{F}_q\) with \(sr \to \infty\) as \(r \to \infty\) and

\[
\lim_{r \to \infty} \frac{tr}{log_q sr} \leq d - 1 - \left\lfloor \frac{d - 1}{q} \right\rfloor.
\]

(5.1)

**Proof.** For each prime \(\ell > (d - 2)!\), let

\[
n(\ell) = q^\ell \quad \text{and} \quad r(\ell) = (d - 2)\ell + \left\lceil \frac{\ell}{d - 1} \right\rceil + 1.
\]

Using [20, Theorem 5] we obtain a linear \([n(\ell), k(\ell), \alpha + 1]\)-code \(C(\ell)\) over \(\mathbb{F}_q\) for each prime \(\ell > (d - 2)\), where \(k(\ell) \geq n(\ell) - r(\ell)\). If \(k(\ell) > n(\ell) - r(\ell)\), then by taking any \((n(\ell) - r(\ell))\)-dimensional \(\mathbb{F}_q\)-linear subspace of \(C(\ell)\), we can assume that \(k(\ell) = n(\ell) - r(\ell)\) without loss of generality. Therefore, by definition of \(M_d(r, q)\), we have

\[
\liminf_{r \to \infty} \frac{r}{log_q M_d(r, q)} \leq \lim_{\ell \to \infty} \frac{r(\ell)}{\ell},
\]
where the last limit is over the prime numbers \( \ell \) satisfying \((d - 2)! < \ell \). Using Lemma 5.1 we conclude that there exists a sequence of digital \((r_r, d, s_r)\)-nets over \( \mathbb{F}_q \) with \( s_r \to \infty \) as \( r \to \infty \) and

\[
\lim_{r \to \infty} \frac{t_r}{\log_q s_r} \leq \lim_{\ell \to \infty} \frac{(d - 2)\ell + \lceil \frac{\ell}{d - 1} \rceil + 1}{\ell} = d - 2 + \frac{1}{d - 1}.
\]

Theorem 5.3 improves Theorem 5.2 if \( \text{char} \, \mathbb{F}_q > d - 2 \) and \( 2 \leq d - 1 < q \). For example if \((q, d) = (7, 7)\) or \((11, 8)\), the upper bounds from Theorem 5.3 are \(31/6\) and \(43/7\), respectively, whereas Theorem 5.2 gives only \(6\) and \(7\), respectively.

Moreover there are some sporadic cases in the literature for which better results than the ones of [20] exist. The results in these sporadic cases are obtained in [3,5,6,8,10]. They are also summarized in [20]. Putting these results, Theorem 3.1, Lemma 5.1, Theorems 5.2 and 5.3 together, we obtain the following.

**Theorem 5.4.** Let \( d \geq 2 \) be an integer and \( q \) be a prime power. In each of the cases below, there exists a sequence of digital \((r_r, d, s_r)\)-nets over \( \mathbb{F}_q \) with \( s_r \to \infty \) as \( r \to \infty \) improving (5.1) as follows:

(i) If \( \text{char} \, \mathbb{F}_q > d - 2 \), then \( \lim_{r \to \infty} \frac{t_r}{\log_q s_r} \leq \min(d - 1 - \lfloor \frac{d - 1}{q} \rfloor, d - 2 + \frac{1}{d - 1}) \).

(ii) If \( (q, d) = (4, 4) \), then \( \lim_{r \to \infty} \frac{t_r}{\log_q s_r} \leq 2 \).

(iii) If \( q \) is a prime power with \( q \geq 5 \) and \( d = 5 \), then \( \lim_{r \to \infty} \frac{t_r}{\log_q s_r} \leq 3 \).

(iv) If \( (q, d) = (3, 5) \), then \( \lim_{r \to \infty} \frac{t_r}{\log_q s_r} \leq \frac{5}{2} \).

(v) If \( (q, d) = (4, 5) \), then \( \lim_{r \to \infty} \frac{t_r}{\log_q s_r} \leq \frac{17}{6} \).

(vi) If \( q \) is a power of 2 with \( q \geq 8 \) and \( d = 4 \), then \( \lim_{r \to \infty} \frac{t_r}{\log_q s_r} \leq \frac{7}{3} \).

(vii) If \( q \) is a prime power with \( q \geq 5 \) and \( d = 3 \), then \( \lim_{r \to \infty} \frac{t_r}{\log_q s_r} \leq \frac{6}{\log_q (q^4 + q^2 - 1)} \).

(viii) If \( (q, d) = (3, 3) \), then \( \lim_{r \to \infty} \frac{t_r}{\log_q s_r} \leq 1.3796 \).

(ix) If \( (q, d) = (4, 3) \), then \( \lim_{r \to \infty} \frac{t_r}{\log_q s_r} \leq 1.45 \).

**Proof.** The proof of item (i) immediately follows from Theorems 5.2 and 5.3. Using Theorem 3.1 we obtain item (ii). The bounds in items (iii), . . . , (ix) follow from [3, Corollary 6], [3, Corollary 7], [8], [3, Theorem 4], [5,6,10], respectively. We explain the details of item (iii) only. The proofs of the other items are similar. For an even integer \( \ell \geq 4 \) let

\[
n(\ell) = q^{[5(\ell - 1)/6]}, \quad r(\ell) = \frac{5}{2} \ell, \quad \text{and} \quad d = 5.
\]

From [3, Corollary 6] we get a linear \([n(\ell), n(\ell) - r(\ell), \geq d + 1]\)-code over \( \mathbb{F}_q \) for each even integer \( \ell \geq 4 \). Then we obtain the bound of item (iii) using Lemma 5.1.

**Remark 5.5.** When \( (q, d) = (4, 4) \), the upper bound 2 in item (ii) of Theorem 5.4 is best possible. Indeed it meets the lower bound of [16, Theorem 9.1]. We recall that Theorem 5.2 and [16, Theorem 9.1] imply other best-possible results in the following cases (cf. [16, Section 9]):
(i) \(q = 2\) and \(d \geq 2\) is an integer,
(ii) \(q\) is an arbitrary prime power and \(d = 2\), and
(iii) \((q, d) = (3, 4)\).

Acknowledgments

We would like to thank the anonymous reviewers for their insightful and useful comments that improved the presentation and quality of the paper.

The authors are partially supported by NTU Research Grant No. M58110003. This paper was written while the second author was visiting Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University. He would like to thank the institution for the hospitality.

References

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