ACTA ARITHMETICA
105.3 (2002)

Constructions of digital nets using global function fields

by

Harald Niederreiter (Singapore)
and Ferruh Özbudak (Ankara)

1. Introduction. The theory of (t, m, s)-nets and (t, s)-sequences provides powerful tools for the construction of low-discrepancy point sets, respectively low-discrepancy sequences, in multidimensional unit cubes. We refer to the monograph [5, Chapter 4] and the recent survey article [6] for general background on this theory. We follow the usual convention in the area that a point set is a multiset in the sense of combinatorics, i.e., that multiplicity of elements is allowed and taken into account.

Definition 1.1. For integers $b \geq 2$, $s \geq 1$, and $0 \leq t \leq m$, a (t, m, s)-*net in base* b is a point set $\mathcal{P}$ consisting of b^m points in $[0, 1)^s$ such that every subinterval of $[0, 1)^s$ of the form

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

with integers $h_i \geq 0$ and $0 \leq k_i < b^{h_i}$ for $1 \leq i \leq s$ and of volume b^{t-m} contains exactly b^t points of $\mathcal{P}$.

The uniformity properties of a (t, m, s)-net in base b are the better the smaller the value of the parameter t. The integer t is often called the *quality parameter* of the net.

In this paper we focus on a special but very important family of nets, namely digital nets. These are nets obtained by the so-called digital construction method. Expository accounts of the theory of digital nets can be found in the book of Niederreiter and Xing [9, Chapter 8] and the survey paper of Larcher [1]. We restrict the attention to the case where the finite ring over which the digital net is constructed is a finite field $\mathbb{F}_q$, where q is

2000 *Mathematics Subject Classification*: 11K38, 11K45, 11R58.

This paper was written while the second author was visiting the Institute for Mathematical Sciences, National University of Singapore, Republic of Singapore. He would like to thank the institute for the support.

an arbitrary prime power. In this case we speak of a *digital* (t, m, s)*-net constructed over* $\mathbb{F}_q$. A digital (t, m, s)-net constructed over $\mathbb{F}_q$ is, in particular, a (t, m, s)-net in base q.

Niederreiter and Pirsic [7] introduced the new viewpoint of duality in the theory of digital nets; see also Skriganov [11] for related work. In this viewpoint, the problem of constructing digital (t, m, s)-nets constructed over $\mathbb{F}_q$ is reduced to that of constructing certain $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^{ms}$. The vector space $\mathbb{F}_q^{ms}$ is endowed with a weight function which generalizes the Hamming weight, and there is then a known relationship between the quality parameter t of the digital net and the minimum distance (or minimum weight) of the corresponding $\mathbb{F}_q$-linear subspace. Small values of t correspond to large values of the minimum distance.

The appropriate weight function on $\mathbb{F}_q^{ms}$ was already introduced by Niederreiter [2] in the theory of low-discrepancy point sets. First, we define a weight function v as follows. For a positive integer m and any vector $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}_q^m$ let $v(\mathbf{a}) = 0$ if $\mathbf{a} = \mathbf{0}$ and $v(\mathbf{a}) = \max\{j : a_j \neq 0\}$ if $\mathbf{a} \neq \mathbf{0}$. Then we extend this definition to $\mathbb{F}_q^{ms}$ by writing a vector $\mathbf{A} \in \mathbb{F}_q^{ms}$ as the concatenation of s vectors of length m, i.e.,

$$\mathbf{A} = (\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(s)}) \in \mathbb{F}_q^{ms} \quad \text{with} \quad \mathbf{a}^{(i)} \in \mathbb{F}_q^m \quad \text{for } 1 \leq i \leq s,$$

and putting

$$V_m(\mathbf{A}) = \sum_{i=1}^{s} v(\mathbf{a}^{(i)}).$$

The following concept is crucial.

Definition 1.2. For any nonzero $\mathbb{F}_q$-linear subspace $\mathcal{N}$ of $\mathbb{F}_q^{ms}$ we define the *minimum distance*

$$\delta_m(\mathcal{N}) = \min_{\mathbf{A} \in \mathcal{N} \setminus \{\mathbf{0}\}} V_m(\mathbf{A}).$$

We apply the approach to the construction of digital nets via duality theory in the context of a construction principle based on global function fields. A construction of digital nets using rational places of global function fields was recently introduced by Niederreiter and Xing [10]. We considerably extend this construction by employing arbitrary places of global function fields. This generalization leads to a greater flexibility and, as a consequence, to improvements on the construction in [10]. The new general construction principle is explained in Section 3. An auxiliary function that is needed in Section 3 is studied in Section 2. Various refinements of the construction in Section 3 are presented in Sections 4 and 5. It is also shown that the same construction principles can be used to obtain so-called (d, k, m, s)-systems over finite fields (see e.g. Theorem 3.7).

2. An auxiliary function. In this section we prove lower bounds on an auxiliary function which we use later in the paper. Let $d_1, \dots, d_s$, and m be positive integers. For each $i = 1, \dots, s$ let m_i and $0 \le r_i < d_i$ be the unique integers satisfying $m = m_i d_i + r_i$. For a given integer $r \ge 0$ let S be the set

$$S := \Big\{(l_1, \dots, l_s) \in \mathbb{Z}^s : \sum_{i=1}^{s} l_i d_i \le r,\ 0 \le l_i \le m_i \text{ for } 1 \le i \le s\Big\}.$$

We define the auxiliary function

$$\delta_m^*(d_1, \dots, d_s; r) := \min\Big\{\sum_{i=1}^{s} \max(0, m - (l_i+1)d_i + 1) : (l_1, \dots, l_s) \in S\Big\}.$$

We will establish lower bounds on $\delta_m^*(d_1, \dots, d_s; r)$. The first bound is an immediate consequence of the definition.

LEMMA 2.1. *For any positive integers $d_1, \dots, d_s$ and m, and any integer $r \ge 0$, we have*

$$\delta_m^*(d_1, \dots, d_s; r) \ge ms - r - \sum_{i=1}^{s} (d_i - 1).$$

Proof. For any $(l_1, \dots, l_s) \in S$ we have

$$\begin{aligned}\sum_{i=1}^{s} \max(0, m - (l_i+1)d_i + 1) &\ge \sum_{i=1}^{s} (m - (l_i+1)d_i + 1) \\ &= ms - \sum_{i=1}^{s} l_i d_i - \sum_{i=1}^{s} (d_i - 1)\end{aligned}$$

and also $\sum_{i=1}^{s} l_i d_i \le r$. This implies the desired bound. ∎

LEMMA 2.2. *With the above notation we have $\delta_m^*(d_1, \dots, d_s; r) \ge 1$ if and only if $r < ms - \sum_{i=1}^{s} r_i$.*

Proof. If $r < ms - \sum_{i=1}^{s} r_i = \sum_{i=1}^{s} m_i d_i$, then for any $(l_1, \dots, l_s) \in S$ we have $l_j \le m_j - 1$ for at least one j with $1 \le j \le s$. Hence

$$\sum_{i=1}^{s} \max(0, m - (l_i+1)d_i + 1) \ge \max(0, m - (l_j+1)d_j + 1) \ge 1,$$

and so $\delta_m^*(d_1, \dots, d_s; r) \ge 1$. If $r \ge ms - \sum_{i=1}^{s} r_i = \sum_{i=1}^{s} m_i d_i$, then $(m_1, \dots, m_s) \in S$, hence

$$\delta_m^*(d_1, \dots, d_s; r) \le \sum_{i=1}^{s} \max(0, m - (m_i+1)d_i + 1) = 0,$$

and so $\delta_m^*(d_1, \dots, d_s; r) = 0$. ∎

Now we establish a lower bound on $\delta_m^*(d_1,\ldots,d_s;r)$ which is at least as good as and in many cases better than that in Lemma 2.1. For $I \subseteq \{1,\ldots,s\}$ we write I' for the complement of I in $\{1,\ldots,s\}$. Using the same notation as in the beginning of this section, we put

$$\mathcal{M}_1 := \Big\{ I \subseteq \{1,\ldots,s\} : \sum_{i\in I'}(m-r_i) \le r,\ \sum_{i\in I} d_i \ge ms - r - \sum_{i=1}^{s} r_i \Big\},$$

$$\mathcal{M}_2 := \Big\{ I \subseteq \{1,\ldots,s\} : \sum_{i\in I'}(m-r_i) \le r,\ \sum_{i\in I} d_i < ms - r - \sum_{i=1}^{s} r_i \Big\}.$$

Furthermore, we set

$$M_1 := \min_{I\in\mathcal{M}_1} \sum_{i\in I}(r_i+1),$$

$$M_2 := ms - r - \sum_{i=1}^{s}(d_i-1) + \min_{I\in\mathcal{M}_2} \sum_{i\in I'}(d_i-1-r_i),$$

where $M_j = \infty$ if $\mathcal{M}_j$ is the empty set ($j = 1, 2$). In view of Lemma 2.2, we can assume $r < ms - \sum_{i=1}^{s} r_i$ in the following result, since otherwise we know that $\delta_m^*(d_1,\ldots,d_s;r) = 0$.

PROPOSITION 2.3. *Let $d_1,\ldots,d_s$ and m be positive integers and for each $i = 1,\ldots,s$ let r_i be the least residue of m modulo d_i. Then for any integer r with $0 \le r < ms - \sum_{i=1}^{s} r_i$ we have*

$$\delta_m^*(d_1,\ldots,d_s;r) \ge \min(M_1, M_2),$$

where M_1 and M_2 are defined above.

Proof. For every nonempty subset I of $\{1,\ldots,s\}$ we put

$$S_I := \Big\{ (l_1,\ldots,l_s) \in \mathbb{Z}^s : \sum_{i=1}^{s} l_i d_i \le r, l_i = m_i \text{ for } i \in I', \\ 0 \le l_i < m_i \text{ for } i \in I \Big\}.$$

Then we have

$$\delta_m^*(d_1,\ldots,d_s;r) = \min_I \min \Big\{ \sum_{i\in I}(m-(l_i+1)d_i+1) : (l_1,\ldots,l_s) \in S_I \Big\}, \tag{2.1}$$

where the outer minimum is over all nonempty subsets I of $\{1,\ldots,s\}$ for which S_I is nonempty. Note that S_I is nonempty if and only if $(k_1,\ldots,k_s) \in S_I$ with $k_i = m_i$ for $i \in I'$ and $k_i = 0$ for $i \in I$, that is, if and only if $\sum_{i\in I'}(m-r_i) \le r$.

Now we consider the inner minimum in (2.1) for a fixed I. We have

$$\min\Big\{\sum_{i\in I}(m-(l_i+1)d_i+1) : (l_1,\dots,l_s)\in S_I\Big\}$$
$$= (m+1)|I| - \sum_{i\in I} d_i - \max\Big\{\sum_{i\in I} l_i d_i : (l_1,\dots,l_s)\in S_I\Big\}.$$

Note that $(l_1,\dots,l_s)\in S_I$ if and only if $(l_i)_{i\in I}\in\mathbb{Z}^{|I|}$ satisfies $0\le l_i<m_i$ for $i\in I$ and

$$\sum_{i\in I} l_i d_i + \sum_{i\in I'} m_i d_i \le r.$$

The last condition is equivalent to

$$\sum_{i\in I} l_i d_i \le r - \sum_{i\in I'}(m-r_i).$$

Therefore we obtain

$$\max\Big\{\sum_{i\in I} l_i d_i : (l_1,\dots,l_s)\in S_I\Big\}$$
$$= \max\Big\{\sum_{i\in I} l_i d_i : (l_i)_{i\in I}\in\mathbb{Z}^{|I|}, \sum_{i\in I} l_i d_i \le r - \sum_{i\in I'}(m-r_i),$$
$$0\le l_i<m_i \text{ for } i\in I\Big\}$$
$$\le \min\Big(r-\sum_{i\in I'}(m-r_i), \sum_{i\in I}(m_i-1)d_i\Big).$$

Note that every nonempty subset I of $\{1,\dots,s\}$ for which S_I is nonempty belongs to either $\mathcal{M}_1$ or $\mathcal{M}_2$. If $I\in\mathcal{M}_1$, then

$$\sum_{i\in I}(m_i-1)d_i = \sum_{i\in I}(m-r_i) - \sum_{i\in I} d_i$$
$$\le \sum_{i\in I}(m-r_i) - ms + r + \sum_{i=1}^{s} r_i$$
$$= \sum_{i\in I}(m-r_i) + r - \sum_{i=1}^{s}(m-r_i) = r - \sum_{i\in I'}(m-r_i),$$

and so

$$\max\Big\{\sum_{i\in I} l_i d_i : (l_1,\dots,l_s)\in S_I\Big\} \le \sum_{i\in I}(m_i-1)d_i.$$

It follows that

$$\min\Big\{\sum_{i\in I}(m-(l_i+1)d_i+1) : (l_1,\ldots,l_s)\in S_I\Big\}$$
$$\geq (m+1)|I| - \sum_{i\in I} d_i - \sum_{i\in I}(m_i-1)d_i$$
$$= (m+1)|I| - \sum_{i\in I}(m-r_i) = \sum_{i\in I}(r_i+1)$$

for all $I\in\mathcal{M}_1$, and so

$$\min_{I\in\mathcal{M}_1}\min\Big\{\sum_{i\in I}(m-(l_i+1)d_i+1) : (l_1,\ldots,l_s)\in S_I\Big\}\geq M_1. \tag{2.2}$$

If $I\in\mathcal{M}_2$, then as above we see that

$$\sum_{i\in I}(m_i-1)d_i > r - \sum_{i\in I'}(m-r_i).$$

Therefore

$$\max\Big\{\sum_{i\in I} l_i d_i : (l_1,\ldots,l_s)\in S_I\Big\}\leq r-\sum_{i\in I'}(m-r_i).$$

It follows that

$$\min\Big\{\sum_{i\in I}(m-(l_i+1)d_i+1) : (l_1,\ldots,l_s)\in S_I\Big\}$$
$$\geq (m+1)|I| - \sum_{i\in I} d_i - r + \sum_{i\in I'}(m-r_i)$$
$$= ms - r - \sum_{i\in I}(d_i-1) - \sum_{i\in I'} r_i$$
$$= ms - r - \sum_{i=1}^{s}(d_i-1) + \sum_{i\in I'}(d_i-1-r_i)$$

for all $I\in\mathcal{M}_2$, and so

$$\min_{I\in\mathcal{M}_2}\min\Big\{\sum_{i\in I}(m-(l_i+1)d_i+1) : (l_1,\ldots,l_s)\in S_I\Big\}\geq M_2. \tag{2.3}$$

By combining (2.1)–(2.3), we obtain the desired result. ∎

Remark 2.4. It is clear that $M_2\geq ms-r-\sum_{i=1}^{s}(d_i-1)$. For $I\in\mathcal{M}_1$ we have

$$\sum_{i\in I}(r_i+1) = \sum_{i=1}^{s}(r_i+1) - \sum_{i\in I'}(r_i+1)$$
$$\geq ms - r - \sum_{i\in I} d_i + s - \sum_{i\in I'}(r_i+1)$$

$$\geq ms - r - \sum_{i\in I} d_i + s - \sum_{i\in I'} d_i = ms - r - \sum_{i=1}^{s}(d_i - 1),$$

and so $M_1 \geq ms - r - \sum_{i=1}^{s}(d_i - 1)$. Therefore

$$\min(M_1, M_2) \geq ms - r - \sum_{i=1}^{s}(d_i - 1),$$

and so the lower bound in Proposition 2.3 is at least as good as that in Lemma 2.1.

REMARK 2.5. If $m \geq d_i$ for $1 \leq i \leq s$, then the condition

$$\sum_{i\in I'}(m - r_i) \leq r$$

in the definition of $\mathcal{M}_1$ is not needed. The reason is that then $m_i \geq 1$ for $1 \leq i \leq s$, and so in view of the inequality

$$\sum_{i\in I}(m_i - 1)d_i \leq r - \sum_{i\in I'}(m - r_i)$$

for $I \in \mathcal{M}_1$, which follows from the second condition in the definition of $\mathcal{M}_1$ (see the proof of Proposition 2.3), we obtain $\sum_{i\in I'}(m - r_i) \leq r$.

EXAMPLE 2.6. It is easy to construct examples in which the lower bound in Proposition 2.3 is better than that in Lemma 2.1. For instance, let $s = 10$, $m = 2$, $r = 17$, $d_1 = d_2 = 2$, and $d_i = 1$ for $3 \leq i \leq 10$. Then $M_1 = 2$, $M_2 = 3$, and so $\delta_2^*(2, 2, 1, 1, 1, 1, 1, 1, 1, 1; 17) \geq 2$ by Proposition 2.3, whereas Lemma 2.1 yields the lower bound 1. If $s = 5$, $m = 6$, $r = 17$, $d_1 = d_2 = 6$, $d_3 = 3$, $d_4 = 2$, $d_5 = 1$, then $M_1 = 3$, $M_2 = 5$, and so $\delta_6^*(6, 6, 3, 2, 1; 17) \geq 3$ by Proposition 2.3, whereas Lemma 2.1 yields the lower bound 0. In both examples it is easily seen that the lower bound in Proposition 2.3 yields the exact value of $\delta_m^*(d_1, \ldots, d_s; r)$.

3. The basic construction. In this section we give our basic construction of $\mathbb{F}_q$-linear subspaces $\mathcal{N}$ of $\mathbb{F}_q^{ms}$ with large minimum distance $\delta_m(\mathcal{N})$. This construction will then be applied to digital nets and so-called (d, k, m, s)-systems.

Let $F/\mathbb{F}_q$ be a global function field with full constant field $\mathbb{F}_q$. Let $P_1, \ldots, P_s$ be $s \geq 1$ distinct places of F with degrees $d_1, \ldots, d_s$, respectively. For each $i = 1, \ldots, s$ let ν_{P_i} be the normalized discrete valuation of F corresponding to P_i and let t_i be a local parameter at P_i. Moreover, for each $i = 1, \ldots, s$ let F_{P_i} be the residue class field of P_i and let $\psi_i : F_{P_i} \to \mathbb{F}_q^{d_i}$ be an $\mathbb{F}_q$-linear vector space isomorphism. Choose an arbitrary divisor G of F and define

$$a_i := \nu_{P_i}(G) \quad \text{for } 1 \leq i \leq s.$$

Let m be an arbitrary positive integer. For each $i = 1, \ldots, s$ we will define an $\mathbb{F}_q$-linear map

$$\theta_i : \mathcal{L}(G) \to \mathbb{F}_q^m$$

on the Riemann–Roch space

$$\mathcal{L}(G) := \{f \in F^* : \mathrm{div}(f) + G \geq 0\} \cup \{0\},$$

where $\mathrm{div}(f)$ denotes the principal divisor of $f \in F^*$. We fix i and repeat the following definitions related to θ_i for each $i = 1, \ldots, s$.

Note that for $f \in \mathcal{L}(G)$ we have $\nu_{P_i}(f) \geq -a_i$, and so the local expansion of f at P_i has the form

$$f = \sum_{j=-a_i}^{\infty} c_{i,j} t_i^j,$$

where all $c_{i,j} \in F_{P_i}$. We denote $c_{i,j}$ by $f^{(j)}(P_i)$. Hence we have

$$\nu_{P_i}\Big(f - \sum_{j=-a_i}^{w} f^{(j)}(P_i) t_i^j\Big) \geq w + 1 \tag{3.1}$$

for any integer $w \geq -a_i$. Let $m_i \geq 0$ and $0 \leq r_i < d_i$ be the unique integers satisfying $m = m_i d_i + r_i$. For $f \in \mathcal{L}(G)$, the image of f under θ_i is defined as

$$\mathbf{c}_f^{(i)} := \theta_i(f) = (0, \ldots, 0, \psi_i(f^{(-a_i+m_i-1)}(P_i)), \ldots, \psi_i(f^{(-a_i)}(P_i))) \in \mathbb{F}_q^m,$$

where we add the r_i-dimensional zero vector $(0, \ldots, 0) \in \mathbb{F}_q^{r_i}$ in the beginning.

Now we set

$$\mathbf{c}_f := (\mathbf{c}_f^{(1)}, \ldots, \mathbf{c}_f^{(s)}) \in \mathbb{F}_q^{ms}$$

and define the $\mathbb{F}_q$-linear map

$$\theta : \mathcal{L}(G) \to \mathbb{F}_q^{ms}, \qquad f \mapsto \mathbf{c}_f.$$

The image of θ is denoted by $C_m(P_1, \ldots, P_s; G)$. Note that, in general, the vector space $C_m(P_1, \ldots, P_s; G)$ depends also on the choice of the local parameters $t_1, \ldots, t_s$ and on the choice of the $\mathbb{F}_q$-linear isomorphisms $\psi_1, \ldots, \psi_s$, but we suppress this dependence in the notation for the sake of simplicity.

We estimate now the dimension and the minimum distance (see Definition 1.2) of the vector space $C_m(P_1, \ldots, P_s; G)$.

THEOREM 3.1. *Let G be a divisor of the global function field $F/\mathbb{F}_q$ with $\dim(\mathcal{L}(G)) \geq 1$ and $\deg(G) < ms - \sum_{i=1}^{s} r_i$. Then the $\mathbb{F}_q$-linear subspace $\mathcal{N} := C_m(P_1, \ldots, P_s; G)$ of $\mathbb{F}_q^{ms}$ has the parameters*

$$\dim(\mathcal{N}) = \dim(\mathcal{L}(G)) \geq \deg(G) + 1 - g,$$
$$\delta_m(\mathcal{N}) \geq \delta_m^*(d_1, \ldots, d_s; \deg(G)),$$

where g is the genus of F.

Proof. For $f \in \mathcal{L}(G) \setminus \{0\}$ put

$$l_i(f) := \min(m_i, \nu_{P_i}(f) + a_i) \geq 0$$

for each $i = 1, \ldots, s$. Then $\nu_{P_i}(f) \geq -a_i + l_i(f)$ and hence

$$f \in \mathcal{L}\Big(G - \sum_{i=1}^{s} l_i(f) P_i\Big).$$

Since $f \neq 0$, we get

$$\begin{aligned} 0 \leq \deg\Big(G - \sum_{i=1}^{s} l_i(f) P_i\Big) &= \deg(G) - \sum_{i=1}^{s} l_i(f) \deg(P_i) \\ &= \deg(G) - \sum_{i=1}^{s} l_i(f) d_i. \end{aligned}$$

Thus, the s-tuple $(l_1(f), \ldots, l_s(f))$ belongs to the set

$$S = \Big\{(l_1, \ldots, l_s) \in \mathbb{Z}^s : \sum_{i=1}^{s} l_i d_i \leq \deg(G),\ 0 \leq l_i \leq m_i \text{ for } 1 \leq i \leq s\Big\}.$$

If $\nu_{P_i}(f) + a_i < m_i$, then $l_i(f) \leq m_i - 1$ and $\nu_{P_i}(f) = -a_i + l_i(f)$, and so by (3.1) we get

$$f^{(-a_i+h)}(P_i) \begin{cases} = 0 & \text{for } 0 \leq h < l_i(f), \\ \neq 0 & \text{for } h = l_i(f). \end{cases}$$

Since ψ_i is an isomorphism, this implies

$$\psi_i(f^{(-a_i+h)}(P_i)) \begin{cases} = \mathbf{0} \in \mathbb{F}_q^{d_i} & \text{for } 0 \leq h < l_i(f), \\ \neq \mathbf{0} \in \mathbb{F}_q^{d_i} & \text{for } h = l_i(f). \end{cases}$$

It follows that

$$v(\mathbf{c}_f^{(i)}) \geq (m_i - l_i(f) - 1)d_i + r_i + 1 = m - (l_i(f) + 1)d_i + 1.$$

If $\nu_{P_i}(f) + a_i \geq m_i$, then $l_i(f) = m_i$ and $\mathbf{c}_f^{(i)} = \mathbf{0} \in \mathbb{F}_q^m$, and so $v(\mathbf{c}_f^{(i)}) = 0$. In all cases we have

$$v(\mathbf{c}_f^{(i)}) \geq \max(0, m - (l_i(f) + 1)d_i + 1).$$

By the definition of $\mathbf{c}_f$ we obtain

$$V_m(\mathbf{c}_f) \geq \sum_{i=1}^{s} \max(0, m - (l_i(f) + 1)d_i + 1).$$

Moreover $(l_1(f), \ldots, l_s(f)) \in S$, and hence we get

$$\begin{aligned} V_m(\mathbf{c}_f) &\geq \min\Big\{\sum_{i=1}^{s} \max(0, m - (l_i + 1)d_i + 1) : (l_1, \ldots, l_s) \in S\Big\} \\ &= \delta_m^*(d_1, \ldots, d_s; \deg(G)) \geq 1 \end{aligned}$$

by Lemma 2.2 and the condition on $\deg(G)$. Therefore the linear map θ is injective and

$$\dim(\mathcal{N}) = \dim(\mathcal{L}(G)) \geq \deg(G) + 1 - g$$

by the Riemann–Roch theorem. The lower bound on $\delta_m(\mathcal{N})$ is immediate from the above. ∎

Now we use Theorem 3.1 and the duality theory for digital nets in [7] to derive digital (t, m, s)-nets constructed over $\mathbb{F}_q$. We can assume $s \geq 2$ to avoid the trivial one-dimensional case.

THEOREM 3.2. *Let $F/\mathbb{F}_q$ be a global function field of genus g. For $s \geq 2$ let $P_1, \ldots, P_s$ be distinct places of F with degrees $d_1, \ldots, d_s$, respectively. Let m be a positive integer and for $i = 1, \ldots, s$ let r_i be the least residue of m modulo d_i. Assume that*

$$m \geq g + \sum_{i=1}^{s} r_i.$$

Then we can obtain a digital (t, m, s)-net constructed over $\mathbb{F}_q$ with

$$t \leq m + 1 - \delta_m^*(d_1, \ldots, d_s; ms - m + g - 1).$$

Proof. We choose a divisor G of F with $\deg(G) = ms - m + g - 1$. Then $\deg(G) < ms - \sum_{i=1}^{s} r_i$ by the given lower bound on m, and also $\dim(\mathcal{L}(G)) \geq \deg(G) + 1 - g \geq 1$ since $s \geq 2$. Therefore we can apply Theorem 3.1 and this yields an $\mathbb{F}_q$-linear subspace $\mathcal{N}$ of $\mathbb{F}_q^{ms}$ with

$$\dim(\mathcal{N}) \geq ms - m, \quad \delta_m(\mathcal{N}) \geq \delta_m^*(d_1, \ldots, d_s; ms - m + g - 1).$$

Now we consider the dual space $\mathcal{C} = \mathcal{N}^{\perp}$ of $\mathcal{N}$ in $\mathbb{F}_q^{ms}$. Then

$$\dim(\mathcal{C}) = ms - \dim(\mathcal{N}) \leq m,$$

and so $\mathcal{C}$ can be viewed as the row space of a suitable $m \times ms$ matrix C over $\mathbb{F}_q$. Finally, we consider the digital net $\mathcal{P}$ with overall generating matrix C (compare with [7, p. 177]). Then [7, Corollary 1] shows that $\mathcal{P}$ is a digital (t, m, s)-net constructed over $\mathbb{F}_q$ with

$$\begin{aligned} t &= m + 1 - \delta_m(\mathcal{C}^{\perp}) = m + 1 - \delta_m(\mathcal{N}) \\ &\leq m + 1 - \delta_m^*(d_1, \ldots, d_s; ms - m + g - 1), \end{aligned}$$

which completes the proof. ∎

COROLLARY 3.3. *Under the conditions of Theorem 3.2, we can obtain a digital (t, m, s)-net constructed over $\mathbb{F}_q$ with*

$$t \leq g + \sum_{i=1}^{s} (d_i - 1).$$

Proof. Combine Theorem 3.2 and Lemma 2.1. ∎

REMARK 3.4. In the special case $d_1 = \ldots = d_s = 1$, the construction leading to Corollary 3.3 was already described in [10]. Since

$$\delta_m^*(1, \ldots, 1; r) = ms - r \quad \text{for } 0 \le r \le ms,$$

Theorem 3.2 yields no improvement on Corollary 3.3 in this case.

REMARK 3.5. We compare the construction of digital nets in this section with a construction in [15] (see also [9, Section 8.4]). In the latter construction we choose $s+1$ distinct places $P_1, \ldots, P_s, P_\infty$ of the global function field $F/\mathbb{F}_q$ with $\deg(P_i) = d_i$ for $1 \le i \le s$ and $\deg(P_\infty) = 1$. In this way we get a digital (t, s)-sequence constructed over $\mathbb{F}_q$ with

$$t = g + \sum_{i=1}^{s} (d_i - 1).$$

By a standard principle (see [9, Lemma 8.2.13]), we obtain then digital $(t, m, s+1)$-nets constructed over $\mathbb{F}_q$ with

$$t = g + \sum_{i=1}^{s} (d_i - 1), \qquad m \ge \max\Big(1, g + \sum_{i=1}^{s} (d_i - 1)\Big).$$

On the other hand, by using the same places $P_1, \ldots, P_s, P_\infty$ in the construction of digital nets described in this section, we obtain digital $(t, m, s+1)$-nets constructed over $\mathbb{F}_q$ with

$$t \le m + 1 - \delta_m^*(d_1, \ldots, d_s, 1; ms + g - 1) \le g + \sum_{i=1}^{s} (d_i - 1)$$

and

$$m \ge \max\Big(1, g + \sum_{i=1}^{s} r_i\Big).$$

Thus, the construction in this section is at least as good as that in [15]. In fact, it is easy to construct examples from Theorem 3.2 which cannot be obtained from [15]. For instance, let $q = 3$ and let F be the rational function field over $\mathbb{F}_3$. Choose the three places of F of degree 2 and the four rational places of F in Theorem 3.2, so that $s = 7$. Furthermore, put $m = 4$ and note that from the definition it is easily seen that $\delta_4^*(2, 2, 2, 1, 1, 1, 1; 23) = 3$. Thus, Theorem 3.2 yields a digital $(t, 4, 7)$-net constructed over $\mathbb{F}_3$ with $t \le 2$. On the other hand, from the construction in [15] using the rational function field F over $\mathbb{F}_3$, the best we can get by any choice of places of F is a digital $(3, 4, 7)$-net constructed over $\mathbb{F}_3$.

The construction in this section also yields so-called (d, k, m, s)-systems. These systems were considered in Niederreiter [3, Section 7], [4] and Niederreiter and Pirsic [7] and are connected with digital nets. For instance, these systems are used in the Kronecker product construction for digital nets

described in [8]. We recall the definition of a (d, k, m, s)-system from [7, Definition 3].

DEFINITION 3.6. Let k, m, s be positive integers and let d be an integer with $0 \le d \le \min(k, ms)$. The system

$$\{\mathbf{c}_j^{(i)} \in \mathbb{F}_q^k : 1 \le j \le m, 1 \le i \le s\}$$

of ms vectors is called a (d, k, m, s)-*system over* $\mathbb{F}_q$ if for any integers h_1, $\ldots, h_s$ with $0 \le h_i \le m$ for $1 \le i \le s$ and $\sum_{i=1}^{s} h_i = d$ the system $\{\mathbf{c}_j^{(i)} \in \mathbb{F}_q^k : 1 \le j \le h_i, 1 \le i \le s\}$ is linearly independent over $\mathbb{F}_q$ (the empty system is considered linearly independent).

It is clear that the value of d depends, in particular, on the specific way in which the ms vectors are arranged into an $s \times m$ array. An important aim in the theory of (d, k, m, s)-systems is to construct, for given q, k, m, and s, a (d, k, m, s)-system over $\mathbb{F}_q$ with d as large as possible. Note that for $k \ge ms$ it is trivial to construct a (d, k, m, s)-system over $\mathbb{F}_q$ with the largest possible value $d = ms$: just take any ms linearly independent vectors from $\mathbb{F}_q^k$ and arrange them in an arbitrary way. Thus, we can assume $k < ms$ in the following. We note that it is also easy to construct a (d, k, m, s)-system over $\mathbb{F}_q$ with $d = k = ms - 1$: let $\mathbf{e}_1, \ldots, \mathbf{e}_k$ be a basis of $\mathbb{F}_q^k$ and arrange the ms vectors $\mathbf{e}_1, \ldots, \mathbf{e}_k, \sum_{b=1}^{k} \mathbf{e}_b$ in an arbitrary way.

THEOREM 3.7. *Let $F/\mathbb{F}_q$ be a global function field of genus g. For $s \ge 1$ let $P_1, \ldots, P_s$ be distinct places of F with degrees $d_1, \ldots, d_s$, respectively. Let m be a positive integer and for $i = 1, \ldots, s$ let r_i be the least residue of m modulo d_i. Let k be an integer with*

$$\max\Big(1, g + \sum_{i=1}^{s} r_i\Big) \le k < ms.$$

Then we can construct a (d, k, m, s)-system over $\mathbb{F}_q$ with

$$d = \delta_m^*(d_1, \ldots, d_s; ms - k + g - 1) - 1 \ge k - g - \sum_{i=1}^{s} (d_i - 1).$$

Proof. We choose a divisor G of F with

$$\deg(G) = ms - k + g - 1.$$

The bounds on k imply that $\deg(G) < ms - \sum_{i=1}^{s} r_i$ and $\dim(\mathcal{L}(G)) \ge \deg(G) + 1 - g \ge 1$. Then Theorem 3.1 yields an $\mathbb{F}_q$-linear subspace $\mathcal{N}$ of $\mathbb{F}_q^{ms}$ with

$$\dim(\mathcal{N}) \ge \deg(G) + 1 - g = ms - k,$$
$$\delta_m(\mathcal{N}) \ge \delta_m^*(d_1, \ldots, d_s; ms - k + g - 1).$$

Now we consider the dual space $\mathcal{C} = \mathcal{N}^{\perp}$ of $\mathcal{N}$ in $\mathbb{F}_q^{ms}$. Then

$$\dim(\mathcal{C}) = ms - \dim(\mathcal{N}) \le k,$$

and so $\mathcal{C}$ can be viewed as the row space of a suitable $k \times ms$ matrix C over $\mathbb{F}_q$. We write

$$C = (C_1|C_2|\dots|C_s),$$

where each submatrix C_i, $1 \le i \le s$, is a $k \times m$ matrix over $\mathbb{F}_q$. Let $\mathbf{c}_1^{(i)}, \dots, \mathbf{c}_m^{(i)} \in \mathbb{F}_q^k$ be the column vectors of C_i. In this way we arrive at the system

$$\{\mathbf{c}_j^{(i)} \in \mathbb{F}_q^k : 1 \le j \le m, 1 \le i \le s\}.$$

The fact that this is a (d, k, m, s)-system over $\mathbb{F}_q$ with

$$d = \delta_m^*(d_1, \dots, d_s; ms - k + g - 1) - 1$$

follows now from [7, Theorem 1], by using $\mathcal{C}^{\perp} = \mathcal{N}$ and the lower bound on $\delta_m(\mathcal{N})$ given above. The lower bound on d is then obtained from Lemma 2.1. ∎

REMARK 3.8. From any (d, k, m, s)-system $\{\mathbf{c}_j^{(i)} \in \mathbb{F}_q^k : 1 \le j \le m, 1 \le i \le s\}$ over $\mathbb{F}_q$ we can obtain a (d, k, m', s)-system over $\mathbb{F}_q$ for any integer $1 \le m' \le m - 1$ satisfying $d \le m's$, by removing the vectors $\mathbf{c}_j^{(i)}$, $m' + 1 \le j \le m$, $1 \le i \le s$, from the system. Similarly, from any (d, k, m, s)-system $\{\mathbf{c}_j^{(i)} \in \mathbb{F}_q^k : 1 \le j \le m, 1 \le i \le s\}$ over $\mathbb{F}_q$ with $d \le m$ we can obtain a (d, k, m', s)-system over $\mathbb{F}_q$ for any integer $m' \ge m + 1$, by adding arbitrary vectors $\mathbf{c}_j^{(i)}$, $m + 1 \le j \le m'$, $1 \le i \le s$, to the system.

EXAMPLE 3.9. For any finite field $\mathbb{F}_q$, it is well known that there exists an elliptic function field E over $\mathbb{F}_q$ with $s = q + \varepsilon + \lfloor 2\sqrt{q} \rfloor$ rational places, where $\varepsilon = 0$ or 1 depending on the form of q (see [9, p. 118]). Let $m \ge 1$ and $1 \le k < ms$ be integers. Then, using all rational places of E, we get a $(k - 1, k, m, s)$-system over $\mathbb{F}_q$ by Theorem 3.7. The special case $k = m$ corresponds to digital $(1, m, q + \varepsilon + \lfloor 2\sqrt{q} \rfloor)$-nets constructed over $\mathbb{F}_q$.

EXAMPLE 3.10. For $q = 8$ consider the function field $F = \mathbb{F}_8(x, y)$ defined by

$$y^7 = x(x + 1)(x^2 + x + 1)^2 = x^6 + x^5 + x^4 + x^3 + x^2 + x.$$

Then F has genus 9 by [12, Corollary III.7.4] and 45 rational places. Furthermore, F has at least one place of degree 2 since $x^2 + x + 1$ is totally ramified in the extension $F/\mathbb{F}_8(x)$. Let $m \ge 1$ and $10 \le k < 46m$ be integers. Then, using all rational places of F and a place of F of degree 2, we get a $(k - 10, k, m, 46)$-system over $\mathbb{F}_8$ by Theorem 3.7. The special case $k = m$ corresponds to digital $(10, m, 46)$-nets constructed over $\mathbb{F}_8$ for all

$m \geq 10$. At present, the smallest known genus among the genera of function fields over $\mathbb{F}_8$ having at least 46 rational places is 11 (see [13]). Hence, using only rational places in the construction in this section, we can get a digital $(t, m, 46)$-net constructed over $\mathbb{F}_8$ only for $t \geq 11$ and $m \geq 11$, no matter which known function field F_1 over $\mathbb{F}_8$ with at least 46 rational places we take. Moreover, for any such function field F_1, if g is its genus, h its divisor class number, and m is so large that $\binom{46+m-g}{45} \geq h$, then we cannot use the improved construction in [10, Section 3] to get digital $(t, m, 46)$-nets constructed over $\mathbb{F}_8$ with $t \leq 10$.

4. An improvement using special $\mathbb{F}_q$-linear isomorphisms. We keep the notation of Section 3. In this section we give an improvement of the construction in Theorem 3.1 by using special $\mathbb{F}_q$-linear isomorphisms ψ_i in the definition of $C_m(P_1, \ldots, P_s; G)$.

First we prove a lemma. For $u \geq 1$ let $e_1, \ldots, e_u \geq 2$ be integers and define the set

$$\mathcal{U} := \{(\varphi_1, \ldots, \varphi_u) : \varphi_i \text{ is an } \mathbb{F}_q\text{-linear automorphism of } \mathbb{F}_q^{e_i} \text{ for } i = 1, \ldots, u\}.$$

LEMMA 4.1. *Let $T \subseteq \prod_{i=1}^{u} (\mathbb{F}_q^{e_i} \setminus \{\mathbf{0}\})$ be a subset of the direct product of the sets $\mathbb{F}_q^{e_i} \setminus \{\mathbf{0}\}$ and $|T| = \mu$. Consider the set*

$$U = \{(\varphi_1, \ldots, \varphi_u) \in \mathcal{U} : \text{for each } (\mathbf{a}_1, \ldots, \mathbf{a}_u) \in T \text{ there exists } i \in \{1, \ldots, u\} \text{ such that } \varphi_i(\mathbf{a}_i) \notin \langle (1, 0, \ldots, 0) \rangle \subseteq \mathbb{F}_q^{e_i}\}.$$

Then

$$|U| \geq \prod_{i=1}^{u} [(q^{e_i} - q)(q^{e_i} - q^2) \ldots (q^{e_i} - q^{e_i - 1})](q-1)^u \times \Big[\prod_{i=1}^{u} (1 + q + \ldots + q^{e_i - 1}) - \mu \Big].$$

In particular, if $\mu < \prod_{i=1}^{u} (1 + q + \ldots + q^{e_i - 1})$, then there exists a u-tuple $(\varphi_1, \ldots, \varphi_u) \in \mathcal{U}$ such that for any $(\mathbf{a}_1, \ldots, \mathbf{a}_u) \in T$ there is at least one $i \in \{1, \ldots, u\}$ with

$$\varphi_i(\mathbf{a}_i) \notin \langle (1, 0, \ldots, 0) \rangle \subseteq \mathbb{F}_q^{e_i}.$$

Proof. We first observe that the cardinality of the set $\mathcal{U}$ is

$$|\mathcal{U}| = \prod_{i=1}^{u} |\{\varphi_i : \varphi_i \text{ is an } \mathbb{F}_q\text{-linear automorphism of } \mathbb{F}_q^{e_i}\}| = \prod_{i=1}^{u} [(q^{e_i} - 1)(q^{e_i} - q) \ldots (q^{e_i} - q^{e_i - 1})].$$

We will consider the complement U' of U in $\mathcal{U}$. For each $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_u) \in T$ let

$$U'_{\mathbf{A}} := \{(\varphi_1, \ldots, \varphi_u) \in \mathcal{U} : \varphi_i(\mathbf{a}_i) \in \langle (1, 0, \ldots, 0) \rangle \text{ for } i = 1, \ldots, u\}.$$

For any $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_u) \in T$, since $\mathbf{a}_i \neq \mathbf{0} \in \mathbb{F}_q^{e_i}$ for $i = 1, \ldots, u$, we have

$$|U'_{\mathbf{A}}| = \prod_{i=1}^{u} [(q-1)(q^{e_i} - q) \ldots (q^{e_i} - q^{e_i - 1})].$$

Moreover, $U' = \bigcup_{\mathbf{A} \in T} U'_{\mathbf{A}}$ by definition and hence

$$|U'| \leq \sum_{\mathbf{A} \in T} |U'_{\mathbf{A}}| = \mu \prod_{i=1}^{u} [(q-1)(q^{e_i} - q) \ldots (q^{e_i} - q^{e_i - 1})].$$

Therefore

$$\begin{aligned} |U| &= |\mathcal{U}| - |U'| \\ &\geq \prod_{i=1}^{u} [(q^{e_i} - 1) \ldots (q^{e_i} - q^{e_i - 1})] - \mu \prod_{i=1}^{u} [(q-1)(q^{e_i} - q) \ldots (q^{e_i} - q^{e_i - 1})] \\ &= \prod_{i=1}^{u} [(q^{e_i} - q) \ldots (q^{e_i} - q^{e_i - 1})](q-1)^u \Big[\prod_{i=1}^{u} (1 + q + \ldots + q^{e_i - 1}) - \mu \Big]. \end{aligned}$$

This finishes the proof. ∎

Remark 4.2. We show that the upper bound on $|T|$ in the second part of Lemma 4.1 cannot be improved in general. We will define a subset $T \subseteq \prod_{i=1}^{u} (\mathbb{F}_q^{e_i} \setminus \{\mathbf{0}\})$ with $T = \prod_{i=1}^{u} (1 + q + \ldots + q^{e_i - 1})$ such that there is no u-tuple $(\varphi_1, \ldots, \varphi_u) \in \mathcal{U}$ having the property in the conclusion of the second part of the lemma. For each $i = 1, \ldots, u$ we define $B_i \subseteq \mathbb{F}_q^{e_i} \setminus \{\mathbf{0}\}$ with $|B_i| = 1 + q + \ldots + q^{e_i - 1}$ as follows. The number of lines passing through the origin in the affine space $\mathbb{F}_q^{e_i}$ is $1 + q + \ldots + q^{e_i - 1}$. For each such line L, we choose a point $\mathbf{p} \in L$ distinct from the origin. Then B_i is the set consisting of these points. Let $T = \{(\mathbf{a}_1, \ldots, \mathbf{a}_u) : \mathbf{a}_i \in B_i \text{ for } i = 1, \ldots, u\}$ and hence $|T| = \prod_{i=1}^{u} |B_i| = \prod_{i=1}^{u} (1 + q + \ldots + q^{e_i - 1})$. Let $(\varphi_1, \ldots, \varphi_u) \in \mathcal{U}$ be arbitrary. For each $i = 1, \ldots, u$ there exists a unique element $\mathbf{b}_i \in B_i$ such that $\varphi_i(\mathbf{b}_i) \in \langle (1, 0, \ldots, 0) \rangle \subseteq \mathbb{F}_q^{e_i}$ by the definition of B_i. Then for $(\mathbf{b}_1, \ldots, \mathbf{b}_u) \in T$ we have $\varphi_i(\mathbf{b}_i) \in \langle (1, 0, \ldots, 0) \rangle \subseteq \mathbb{F}_q^{e_i}$ for $i = 1, \ldots, u$. Hence for this subset T, the property in the conclusion of the second part of the lemma is not satisfied.

Recall from Section 2 that

$$S = \Big\{ (l_1, \ldots, l_s) \in \mathbb{Z}^s : \sum_{i=1}^{s} l_i d_i \leq r,\ 0 \leq l_i \leq m_i \text{ for } 1 \leq i \leq s \Big\}.$$

As in Section 3 we let $r = \deg(G)$ and we now define a "minimal" subset $S_{\min}$ of S as

$$S_{\min} := \Big\{(l_1, \ldots, l_s) \in S : \sum_{i=1}^{s} \max(0, m - (l_i + 1)d_i + 1) = \delta_m^*(d_1, \ldots, d_s; \deg(G))\Big\}.$$

First, for simplicity, we assume that for any $(l_1, \ldots, l_s) \in S_{\min}$ we have $\sum_{i=1}^{s} l_i d_i = \deg(G)$. Moreover, we also assume that for any $(l_1, \ldots, l_s) \in S_{\min}$ and any $i \in \{1, \ldots, s\}$, if $d_i \geq 2$, then $l_i < m_i$. For some interesting cases these assumptions are valid.

THEOREM 4.3. *Under the notation and the assumptions as above, if*

$$|S_{\min}| < \prod_{i=1}^{s} (1 + q + \ldots + q^{d_i - 1}),$$

then there exist $\mathbb{F}_q$-linear isomorphisms $\widetilde{\psi}_i : F_{P_i} \to \mathbb{F}_q^{d_i}$ for $i = 1, \ldots, s$ such that, using these $\mathbb{F}_q$-linear isomorphisms in the definition of θ, for the resulting vector space $\mathcal{N} = C_m(P_1, \ldots, P_s; G)$ we have

$$\delta_m(\mathcal{N}) \geq \delta_m^*(d_1, \ldots, d_s; \deg(G)) + 1.$$

Proof. Let $\mathcal{D}_{\min}$ be the set of the divisors of F corresponding to $S_{\min}$, defined as

$$\mathcal{D}_{\min} := \{l_1 P_1 + \ldots + l_s P_s : (l_1, \ldots, l_s) \in S_{\min}\}.$$

In view of the proof of Theorem 3.1, it is enough to prove that there is a choice of isomorphisms $\widetilde{\psi}_1, \ldots, \widetilde{\psi}_s$ such that for any $D \in \mathcal{D}_{\min}$ and $f \in \mathcal{L}(G - D) \setminus \{0\}$ we have

$$V_m(\mathbf{c}_f) \geq \delta_m^*(d_1, \ldots, d_s; \deg(G)) + 1.$$

For any $D \in \mathcal{D}_{\min}$ we have $\deg(D) = \deg(G)$ by one of our assumptions. Therefore $\dim(\mathcal{L}(G - D)) \leq 1$ by Clifford's theorem [12, Theorem I.6.11]. We can assume $\dim \mathcal{L}(G - D) = 1$ for each $D \in \mathcal{D}_{\min}$ without loss of generality, otherwise we can remove the corresponding D from $\mathcal{D}_{\min}$ and the corresponding $(l_1, \ldots, l_s)$ from $S_{\min}$. For each $D \in \mathcal{D}_{\min}$ we choose a nonzero function $f_D \in \mathcal{L}(G - D)$ and let $\mathcal{M} = \{f_D : D \in \mathcal{D}_{\min}\}$ be the set of these functions. Therefore for any $f_D \in \mathcal{M}$, if $D = \sum_{i=1}^{s} l_i P_i$, then $\nu_{P_i}(f_D) = l_i - \nu_{P_i}(G)$ for $i = 1, \ldots, s$. Note that $|\mathcal{M}| \leq |S_{\min}|$ and that it suffices to prove that

$$V_m(\mathbf{c}_f) \geq \delta_m^*(d_1, \ldots, d_s; \deg(G)) + 1 \quad \text{for any } f \in \mathcal{M}.$$

With the notation in Section 3, for $f \in \mathcal{M}$ and chosen local parameters t_i at P_i and $\mathbb{F}_q$-linear vector space isomorphisms $\psi_i : F_{P_i} \to \mathbb{F}_q^{d_i}$ for $i = 1, \ldots, s$,

let

$$\boldsymbol{\alpha}_{i,f} := \psi_i(f^{(\nu_{P_i}(f))}(P_i)) \in \mathbb{F}_q^{d_i} \setminus \{\mathbf{0}\}$$

for those $i = 1, \dots, s$ with $d_i \geq 2$. Consider the set

$$T = \Big\{(\boldsymbol{\alpha}_{i,f}) \in \prod_{\substack{i=1 \\ d_i \geq 2}}^{s} (\mathbb{F}_q^{d_i} \setminus \{\mathbf{0}\}) : f \in \mathcal{M}\Big\}.$$

By assumption, $|S_{\min}| < \prod_{i=1}^{s}(1 + q + \ldots + q^{d_i - 1})$. Then we have

$$|T| \leq |\mathcal{M}| \leq |S_{\min}| < \prod_{i=1}^{s}(1 + q + \ldots + q^{d_i-1}) = \prod_{\substack{i=1 \\ d_i \geq 2}}^{s} (1 + q + \ldots + q^{d_i-1}).$$

Therefore we can apply the second part of Lemma 4.1. This yields an $\mathbb{F}_q$-linear automorphism φ_i of $\mathbb{F}_q^{d_i}$ for each $i = 1, \dots, s$ with $d_i \geq 2$ such that the following holds: for each $f \in \mathcal{M}$ there exists $i \in \{1, \dots, s\}$ with $d_i \geq 2$ satisfying

$$\varphi_i(\boldsymbol{\alpha}_{i,f}) \notin \langle (1, 0, \dots, 0) \rangle \subseteq \mathbb{F}_q^{d_i}.$$

Moreover, $\nu_{P_i}(f) + \nu_{P_i}(G) = l_i \leq m_i - 1$ by assumption, and hence $\boldsymbol{\alpha}_{i,f}$ is a part of $\mathbf{c}_f^{(i)}$ in the definition of θ_i. Therefore, using the $\mathbb{F}_q$-linear isomorphisms $\widetilde{\psi}_i : F_{P_i} \to \mathbb{F}_q^{d_i}$ given by

$$\widetilde{\psi}_i = \begin{cases} \varphi_i \circ \psi_i & \text{if } d_i \geq 2, \\ \psi_i & \text{if } d_i = 1, \end{cases} \qquad \text{for } i = 1, \dots, s$$

in the definition of θ, we get indeed

$$V_m(\mathbf{c}_f) \geq \delta_m^*(d_1, \dots, d_s; \deg(G)) + 1 \quad \text{for any } f \in \mathcal{M}.$$

This finishes the proof. ∎

Now we give an example illustrating Theorem 4.3.

EXAMPLE 4.4. Let $q = 2$ and let $F = \mathbb{F}_2(x)$ be the rational function field over $\mathbb{F}_2$. Let P_1, P_2, P_∞, and Q be the places of F which are the zeros of the functions $x, x+1, 1/x$, and x^2+x+1, respectively. Assume that local parameters at P_1, P_2, P_∞, Q and $\mathbb{F}_q$-linear isomorphisms $\psi_1 : F_{P_1} \to \mathbb{F}_2$, $\psi_2 : F_{P_2} \to \mathbb{F}_2$, $\psi_3 : F_{P_\infty} \to \mathbb{F}_2$, $\psi_4 : F_Q \to \mathbb{F}_2^2$ are chosen arbitrarily. By Theorem 3.1, for $\mathcal{N} = C_2(P_1, P_2, P_\infty, Q; 6P_\infty)$ we have $\delta_2(\mathcal{N}) \geq \delta_2^*(1, 1, 1, 2; 6) = 1$. Moreover, $S_{\min} = \{(2, 2, 2, 0)\}$ and the assumptions of Theorem 4.3 are satisfied. Note that $\mathcal{L}(6P_\infty - 2P_1 - 2P_2 - 2P_\infty) = \{0, f\}$ with $f = x^2(x+1)^2 \equiv 1 \bmod Q$. Let $\boldsymbol{\alpha} = \psi_4(1) \in \mathbb{F}_2^2 \setminus \{(0,0)\}$ and $\boldsymbol{\beta} = \psi_4(\xi) \in \mathbb{F}_2^2 \setminus \{(0,0)\}$, where $\xi \equiv x \bmod Q$. Let $\varphi_4 : \mathbb{F}_2^2 \to \mathbb{F}_2^2$ be defined as $\varphi_4(\boldsymbol{\alpha}) = (0, 1)$ and $\varphi_4(\boldsymbol{\beta}) = (1, 0)$. Hence, using the $\mathbb{F}_2$-linear isomorphisms $\widetilde{\psi}_1 = \psi_1$, $\widetilde{\psi}_2 = \psi_2$, $\widetilde{\psi}_3 = \psi_3$, and $\widetilde{\psi}_4 = \varphi_4 \circ \psi_4$ for defining θ in the definition of $C_2(P_1, P_2, P_\infty, Q; 6P_\infty)$,

we get $\delta_2(\mathcal{N}) \geq 2$ by Theorem 4.3. Since this lower bound is best possible by the generalized Singleton bound [7, Proposition 1], we obtain $\delta_2(\mathcal{N}) = 2$.

REMARK 4.5. It is possible to generalize Theorem 4.3 to the case where for some $(l_1, \ldots, l_s) \in S_{\min}$ we have $\sum_{i=1}^{s} l_i d_i < \deg(G)$. First we generalize Lemma 4.1 in the following sense. For integers $u, \mu, B \geq 1$ and $e_1, \ldots, e_u \geq B + 1$, let $V_{i,1}, \ldots, V_{i,\mu} \subseteq \mathbb{F}_q^{e_i}$ be given $\mathbb{F}_q$-linear subspaces of dimension at most B for $i = 1, \ldots, u$. By a counting argument, for q large enough, there is a u-tuple $(\varphi_1, \ldots, \varphi_u) \in \mathcal{U}$ such that for each $j = 1, \ldots, \mu$ there exists $i \in \{1, \ldots, u\}$ with $(1, 0, \ldots, 0) \in \mathbb{F}_q^{e_i} \setminus \varphi_i(V_{i,j})$. Note that it is important to have an effective lower bound on q as in Lemma 4.1. Now we can generalize Theorem 4.3. Recall that if D is any divisor of F with $0 \leq \deg(D) \leq 2g - 2$, then $\dim(\mathcal{L}(D)) \leq 1 + (1/2)\deg(D)$ by Clifford's theorem. Also, if $\deg(D) \geq \max(0, 2g - 1)$, then $\dim(\mathcal{L}(D)) = \deg(D) + 1 - g$ by the Riemann–Roch theorem. Hence there is an effective upper bound B on the set $\{\dim(\mathcal{L}(G - l_1P_1 - \ldots - l_sP_s)) : (l_1, \ldots, l_s) \in S_{\min}\}$. Indeed let

$$d = \max\Bigl\{\deg(G) - \sum_{i=1}^{s} l_i d_i : (l_1, \ldots, l_s) \in S_{\min}\Bigr\}.$$

Note that $d \geq 0$ and

$$B = \begin{cases} 1 + d/2 & \text{if } d \leq 2g - 2, \\ d + 1 - g & \text{if } d \geq 2g - 1, \end{cases}$$

is an upper bound. Moreover, for certain divisors G of F and $d \leq 2g - 2$, we can also improve the bound B depending on G in some cases. Now assume that there exists $i \in \{1, \ldots, s\}$ with $d_i \geq B + 1$. Also assume that for any $(l_1, \ldots, l_s) \in S_{\min}$ and any $i \in \{1, \ldots, s\}$, if $d_i \geq B + 1$, then $l_i < m_i$. Therefore, if q is large enough, using the generalized version of Lemma 4.1 and similar arguments as in the proof of Theorem 4.3, we obtain that there exist $\mathbb{F}_q$-linear isomorphisms $\widetilde{\psi}_i : F_{P_i} \to \mathbb{F}_q^{d_i}$ for $i = 1, \ldots, s$ such that using these $\mathbb{F}_q$-linear isomorphisms in the definition of θ instead of arbitrary $\mathbb{F}_q$-linear isomorphisms, for $\mathcal{N} = C_m(P_1, \ldots, P_s; G)$ we have $\delta_m(\mathcal{N}) \geq \delta_m^*(d_1, \ldots, d_s; \deg(G)) + 1$.

Note that $S_{\min}$ is independent of q and an explicit knowledge of $S_{\min}$ allows us to have weaker assumptions in some cases and also to get an effective lower bound on q for the generalized version of Lemma 4.1 above and for other suitable generalizations or improvements of the lemma.

It is clear that by proceeding as in the proofs of Theorems 3.2 and 3.7, we can obtain improved parameters in digital (t, m, s)-nets constructed over $\mathbb{F}_q$ and (d, k, m, s)-systems over $\mathbb{F}_q$ under the conditions of Theorem 4.3 and Remark 4.5.

5. An improvement using a distinguished divisor. In this section we improve our basic construction of Section 3 by choosing a distinguished divisor G of the global function field F. We use a generalized version of a similar idea of Niederreiter and Xing [10, Section 3] which is in turn based on an idea introduced by Xing [14] in the theory of algebraic-geometry codes.

We keep the notation of previous sections. We also assume that F has a rational place Q, for simplicity. Let h be the divisor class number of F and for $i \geq 0$ let A_i denote the number of positive divisors of F of degree i. We also put $A_i = 0$ for $i < 0$. First we prove a lemma.

LEMMA 5.1. *Let $U_1, \ldots, U_l$ be sets of divisors of F of degree $u_1, \ldots, u_l$, respectively. If r is an integer with*

$$\sum_{i=1}^{l} |U_i| \cdot A_{r-u_i} < h,$$

then there exists a divisor G of F of degree r such that

$$\mathcal{L}(G - D) = \{0\} \quad \text{for all } D \in \bigcup_{i=1}^{l} U_i.$$

Proof. Since $\mathcal{L}(B) = \{0\}$ for any divisor B of F with $\deg(B) < 0$, we can restrict the attention to the case where $r \geq \max(u_1, \ldots, u_l)$. For $i = 1, \ldots, l$ let

$$\mathcal{E}_i = \{(D_i, E_i) : D_i \in U_i \text{ and } E_i \text{ is a positive divisor of } F \text{ of degree } r - u_i\},$$

and put $\mathcal{E} = \bigcup_{i=1}^{l} \mathcal{E}_i$. Then $|\mathcal{E}_i| = |U_i| \cdot A_{r-u_i}$, $|\mathcal{E}| \leq \sum_{i=1}^{l} |U_i| \cdot A_{r-u_i}$, and

$$\mathcal{E} = \Big\{(D, E) : D \in \bigcup_{i=1}^{l} U_i \text{ and } E \text{ is a positive divisor of } F \text{ of degree } r - \deg(D)\Big\}.$$

Assume that $\sum_{i=1}^{l} |U_i| \cdot A_{r-u_i} < h$. Recall that the set of degree zero divisors of F is divided into h disjoint subsets by the equivalence relation between the divisors. The set $\widetilde{\mathcal{E}} = \{D + E - rQ : (D, E) \in \mathcal{E}\}$ is a subset of the set of degree zero divisors of F. Moreover, $|\widetilde{\mathcal{E}}| \leq |\mathcal{E}| \leq \sum_{i=1}^{l} |U_i| \cdot A_{r-u_i} < h$, and hence there exists a degree zero divisor H_0 of F such that

$$H_0 \not\sim H \quad \text{for all } H \in \widetilde{\mathcal{E}}.$$

For such a divisor H_0, let $G = H_0 + rQ$. We claim that $\mathcal{L}(G - D) = \{0\}$ for any $D \in \bigcup_{i=1}^{l} U_i$, which finishes the proof. Otherwise, for some $1 \leq i \leq l$ there exist $D \in U_i$ and $f \in \mathcal{L}(G - D) \setminus \{0\}$. Then we have $E := G - D + \operatorname{div}(f) \geq 0$, $\deg(E) = r - u_i$, and $D + E - rQ \in \widetilde{\mathcal{E}}$. Therefore

$$H_0 = G - rQ = D + E - rQ - \mathrm{div}(f) \sim D + E - rQ,$$

which is a contradiction to the definition of H_0. ∎

We need some notation and definitions to give the improved construction of this section. First recall from Section 2 that with the notation introduced there we have

$$S = \Big\{(l_1, \ldots, l_s) \in \mathbb{Z}^s : \sum_{i=1}^{s} l_i d_i \le r,\ 0 \le l_i \le m_i \text{ for } 1 \le i \le s\Big\}$$

and

$$\delta_m^*(d_1, \ldots, d_s; r) = \min\Big\{\sum_{i=1}^{s} \max(0, m - (l_i+1)d_i + 1) : (l_1, \ldots, l_s) \in S\Big\}.$$

For integers $u \ge 0$ let

$$S_{\min}(u,u) := \Big\{(l_1, \ldots, l_s) \in S : \sum_{i=1}^{s} \max(0, m - (l_i+1)d_i + 1) = \delta_m^*(d_1, \ldots, d_s; r) + u\Big\}.$$

Note that $S_{\min}(0,0) = S_{\min}$, which was defined in Section 4. For integers $u \ge 1$ and $0 \le v \le u-1$ we define $S_{\min}(u,v)$ to be the set of $(l_1, \ldots, l_s) \in S_{\min}(v,v)$ such that there is no $(l_1', \ldots, l_s') \in S$ with $(l_1', \ldots, l_s') \ne (l_1, \ldots, l_s)$, $l_i' \le l_i$ for $1 \le i \le s$, and

$$\sum_{i=1}^{s} \max(0, m - (l_i'+1)d_i + 1) \le \delta_m^*(d_1, \ldots, d_s; r) + u.$$

We show that the cardinalities of the sets $S_{\min}(u,v)$ are small for small values of v.

LEMMA 5.2. *With the notation as above let $u \ge 1$. For $d \ge 1$, if $0 \le v \le u-d$, then*

$$(l_1, \ldots, l_s) \in S_{\min}(u,v) \Rightarrow l_i = 0 \text{ for each } i \in \{1, \ldots, s\} \text{ with } d_i \le d.$$

In particular, if $d = \max(d_1, \ldots, d_s)$, then $S_{\min}(u,v) \subseteq \{(0, \ldots, 0)\}$ for any $0 \le v \le u-d$. Moreover, if also $S_{\min}(u,u) \ne \emptyset$ or $u < (m+1)s - \sum_{i=1}^{s} d_i - \delta_m^*(d_1, \ldots, d_s; r) + d$, then $S_{\min}(u,v) = \emptyset$ for any $0 \le v \le u-d$.

Proof. We proceed by contradiction. First assume that $d \ge 1$, $0 \le v \le u-d$, $(l_1, \ldots, l_s) \in S_{\min}(u,v)$, and $l_{i_0} \ge 1$ for some $1 \le i_0 \le s$ with $d_{i_0} \le d$. Let $l_i' = l_i$ for $i \ne i_0$ and $i \in \{1, \ldots, s\}$ and $l_{i_0}' = l_{i_0} - 1$. It is clear that $(l_1', \ldots, l_s') \in S$. If $l_{i_0} = m_{i_0}$, then

$$\sum_{i=1}^{s}\max(0,m-(l_i'+1)d_i+1)=\sum_{i=1}^{s}\max(0,m-(l_i+1)d_i+1)+r_{i_0}+1$$
$$=\delta_m^*(d_1,\dots,d_s;r)+v+r_{i_0}+1$$
$$\le\delta_m^*(d_1,\dots,d_s;r)+u.$$

Moreover, $l_i'\le l_i$ for all $i=1,\dots,s$, and hence we get a contradiction to the definition of $S_{\min}(u,v)$. Similarly, if $1\le l_{i_0}\le m_{i_0}-1$, then

$$\sum_{i=1}^{s}\max(0,m-(l_i'+1)d_i+1)=\sum_{i=1}^{s}\max(0,m-(l_i+1)d_i+1)+d_{i_0}$$
$$=\delta_m^*(d_1,\dots,d_s;r)+v+d_{i_0}$$
$$\le\delta_m^*(d_1,\dots,d_s;r)+u.$$

Therefore this also gives a contradiction, and so the first part of the lemma is shown.

Now for $u\ge 1$, $d=\max(d_1,\dots,d_s)$, and $0\le v\le u-d$ assume that $(0,\dots,0)\in S_{\min}(u,v)$. Then

$$\sum_{i=1}^{s}\max(0,m-(0+1)d_i+1)=(m+1)s-\sum_{i=1}^{s}d_i=\delta_m^*(d_1,\dots,d_s;r)+v.$$

Therefore

$$u\ge v+d=(m+1)s-\sum_{i=1}^{s}d_i-\delta_m^*(d_1,\dots,d_s;r)+d.$$

Furthermore, for any $(l_1,\dots,l_s)\in S$ we have

$$\sum_{i=1}^{s}\max(0,m-(l_i+1)d_i+1)\le\sum_{i=1}^{s}\max(0,m-(0+1)d_i+1)$$
$$=\delta_m^*(d_1,\dots,d_s;r)+v$$
$$<\delta_m^*(d_1,\dots,d_s;r)+u,$$

and so $S_{\min}(u,u)=\emptyset$. ∎

Remark 5.3. By the preceding lemma, for $u\ge 1$ and $d_1=\ldots=d_s=1$, if

$$u\le\min(ms,r)=ms-\max(0,ms-r)=(m+1)s-\sum_{i=1}^{s}1-\delta_m^*(1,\dots,1;r),$$

then $S_{\min}(u,v)=\emptyset$ for any $0\le v\le u-1$.

Example 5.4. We give simple examples for which $u\ge 1$, $0\le v\le u-1$, and $S_{\min}(u,v)\ne\emptyset$. Let $s=2$, $d_1=1$, $d_2=2$, and $m=4$. First, for $r=4$ we have $\delta_4^*(1,2;4)=3$, $S_{\min}(3,3)=\{(1,0)\}$, $S_{\min}(3,2)=\{(0,1)\}$, and $S_{\min}(3,1)=S_{\min}(3,0)=\emptyset$. Second, for $r=2$ we have $\delta_4^*(1,2;2)$

$= 5$, $S_{\min}(4,4) = S_{\min}(4,3) = \emptyset$, $S_{\min}(4,2) = \{(0,0)\}$, and $S_{\min}(4,1) = S_{\min}(4,0) = \emptyset$. Note that in this case $d = \max(1,2) = 2$ and $u = 4 \geq (m+1)s - \sum_{i=1}^{s} d_i - \delta_m^*(d_1,\ldots,d_s;r) + d = 5 \cdot 2 - (1+2) - 5 + 2$.

Now we partition the sets $S_{\min}(u,v)$ into subsets $T(u,v;\lambda)$ such that for any $(l_1,\ldots,l_s) \in T(u,v;\lambda)$ we have $\sum_{i=1}^{s} l_i d_i = \lambda$. First, for $0 \leq v \leq u$ and $S_{\min}(u,v) \neq \emptyset$ we define

$$\Delta(u,v) := \max\Big\{ \sum_{i=1}^{s} l_i d_i : (l_1,\ldots,l_s) \in S_{\min}(u,v) \Big\}.$$

Then for $0 \leq v \leq u$ and $0 \leq \lambda \leq \Delta(u,v)$ we let

$$T(u,v;\lambda) := \Big\{ (l_1,\ldots,l_s) \in S_{\min}(u,v) : \sum_{i=1}^{s} l_i d_i = \lambda \Big\}.$$

If $S_{\min}(u,v) = \emptyset$, then we put $\Delta(u,v) := 0$ and $T(u,v;0) := \emptyset$. Now we can establish the following improvement on Theorem 3.1.

THEOREM 5.5. *With the notation as above, if $r \geq 0$, $u \geq 0$, and*

$$\sum_{v=0}^{u} \sum_{\lambda=0}^{\Delta(u,v)} |T(u,v;\lambda)| \cdot A_{r-\lambda} < h,$$

then there exists a divisor G of F such that $\deg(G) = r$ and either $\mathcal{L}(G) = \{0\}$ or

$$\delta_m(C_m(P_1,\ldots,P_s;G)) \geq \delta_m^*(d_1,\ldots,d_s;r) + u + 1.$$

Proof. First observe that for divisors $D_1 \leq D_2$, if G is any divisor satisfying $\mathcal{L}(G - D_1) = \{0\}$, then we have $\mathcal{L}(G - D_2) = \{0\}$. For a given $u \geq 0$ let

$$S(u) = \Big\{ (l_1,\ldots,l_s) \in S : \sum_{i=1}^{s} \max(0, m - (l_i+1)d_i + 1) \leq \delta_m^*(d_1,\ldots,d_s;r) + u \Big\}.$$

By the definition of $T(u,v;\lambda)$, the set

$$T(u) := \bigcup_{v=0}^{u} \bigcup_{\lambda=0}^{\Delta(u,v)} T(u,v;\lambda) = \bigcup_{v=0}^{u} S_{\min}(u,v)$$

is a subset of $S(u)$ such that for any $(l_1,\ldots,l_s) \in S(u)$, there exists $(l_1',\ldots,l_s') \in T(u)$ having the property that $l_i' \leq l_i$ for all $i = 1,\ldots,s$. Therefore, by the observation at the beginning of the proof and Lemma 5.1, there exists a divisor G of F with $\deg(G) = r$ satisfying

$$\mathcal{L}(G - (l_1P_1 + \ldots + l_sP_s)) = \{0\} \quad \text{for all } (l_1,\ldots,l_s) \in S(u).$$

Hence if $\dim(\mathcal{L}(G)) \geq 1$, then

$$\delta_m(C_m(P_1, \ldots, P_s; G)) \geq \delta_m^*(d_1, \ldots, d_s; r) + u + 1$$

by the proof of Theorem 3.1 and the definition of $S(u)$. ∎

REMARK 5.6. We can rule out the case $\mathcal{L}(G) = \{0\}$ in the conclusion of Theorem 5.5 by imposing the condition $r \geq g$, where g is the genus of F.

REMARK 5.7. We can combine the method of Section 4 with the preceding theorem in order to relax the conditions of the theorem. For instance, let $r \geq 0$, $u = 0$, and $T(0) = \bigcup_{\lambda=0}^{\Delta(0,0)} T(0, 0; \lambda)$ be the set defined as in the proof of Theorem 5.5. Assume that there exists a subset $T_0 \subseteq T(0)$ satisfying the following:

(i) $(l_1, \ldots, l_s) \in T_0 \Rightarrow \sum_{i=1}^{s} l_i d_i = r$,
(ii) $|T_0| < \prod_{i=1}^{s}(1 + q + \ldots + q^{d_i - 1})$, and
(iii) $|T(0) \setminus T_0| + \sum_{\lambda=0,\, \lambda \neq r}^{\Delta(0,0)} |T(0, 0; \lambda)| \cdot A_{r-\lambda} < h$.

Then there exist a divisor G of F with $\deg(G) = r$ and $\mathbb{F}_q$-linear isomorphisms $\widetilde{\psi}_i : F_{P_i} \to \mathbb{F}_q^{d_i}$ for $i = 1, \ldots, s$ such that, using these $\mathbb{F}_q$-linear isomorphisms in the definition of θ, for $\mathcal{N} = C_m(P_1, \ldots, P_s; G)$ we have $\delta_m(\mathcal{N}) \geq \delta_m^*(d_1, \ldots, d_s; r) + 1$.

References

[1] G. Larcher, *Digital point sets: analysis and application*, in: Random and Quasi-Random Point Sets, P. Hellekalek and G. Larcher (eds.), Lecture Notes in Statist. 138, Springer, New York, 1998, 167–222.

[2] H. Niederreiter, *Low-discrepancy point sets*, Monatsh. Math. 102 (1986), 155–167.

[3] —, *Point sets and sequences with small discrepancy*, ibid. 104 (1987), 273–337.

[4] —, *A combinatorial problem for vector spaces over finite fields*, Discrete Math. 96 (1991), 221–228.

[5] —, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, 1992.

[6] —, *Constructions of* (t, m, s)*-nets*, in: Monte Carlo and Quasi-Monte Carlo Methods 1998, H. Niederreiter and J. Spanier (eds.), Springer, Berlin, 2000, 70–85.

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

[8] —, —, *A Kronecker product construction for digital nets*, in: Monte Carlo and Quasi-Monte Carlo Methods 2000, K.-T. Fang, F. J. Hickernell, and H. Niederreiter (eds.), Springer, Berlin, 2002, 396–405.

[9] H. Niederreiter and C. P. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications*, London Math. Soc. Lecture Note Ser. 285, Cambridge Univ. Press, Cambridge, 2001.

[10] —, —, *A construction of digital nets with good asymptotic behavior*, Technical Report, Temasek Laboratories, National University of Singapore, 2001.

[11] M. M. Skriganov, *Coding theory and uniform distributions*, Algebra i Analiz 13 (2001), 191–239 (in Russian).

[12] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.
[13] G. van der Geer and M. van der Vlugt, *Tables of curves with many points*, available at http://www.science.uva.nl/~geer/tables-mathcomp10.ps.
[14] C. P. Xing, *Algebraic-geometry codes with asymptotic parameters better than the Gilbert–Varshamov and the Tsfasman–Vlăduţ–Zink bounds*, IEEE Trans. Inform. Theory 47 (2001), 347–352.
[15] C. P. Xing and H. Niederreiter, *A construction of low-discrepancy sequences using global function fields*, Acta Arith. 73 (1995), 87–102.

Department of Mathematics
National University of Singapore
2 Science Drive 2
Singapore 117543, Republic of Singapore
E-mail: nied@math.nus.edu.sg

Department of Mathematics
Middle East Technical University
İnönü Bulvarı
06531 Ankara, Turkey
E-mail: ozbudak@math.metu.edu.tr

Received on 25.2.2002 (4237)