ACTA ARITHMETICA
XCVII.2 (2001)

Duality for digital nets and its applications

by

Harald Niederreiter and Gottlieb Pirsic (Wien)

1. Introduction. The theory of (t, m, s)-nets provides powerful tools for the construction of low-discrepancy point sets in the s-dimensional unit cube. We refer to the monograph [7] and to the recent survey [8] for a general background on (t, m, s)-nets. Throughout this paper, we assume that the dimension $s \geq 1$ is fixed and 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. For integers $b \geq 2$ 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

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

with integers $d_i \geq 0$ and $0 \leq a_i < b^{d_i}$ for $1 \leq i \leq s$ and of volume b^{t-m} contains exactly b^t points of $\mathcal{P}$. Furthermore, $\mathcal{P}$ is a *strict (t, m, s)-net in base b* if t is the least value u such that $\mathcal{P}$ is a (u, m, s)-net in base b.

Remark 1. The uniformity properties of a (t, m, s)-net in base b are the better the smaller the value of the parameter t. For this reason, t is often called the *quality parameter* of the net. The term *b-ary box* is used for the subintervals of $[0, 1)^s$ considered in Definition 1.

In this paper we focus on a special family of nets, namely digital nets (see Definition 4 below). Most known constructions of nets actually yield digital nets, and digital nets have a particularly nice theory. The leitmotif of the present work is an analogy between digital nets and linear codes that was already observed in [5, Remark 7.13] and further exploited among others by Adams and Shader [1], Lawrence *et al.* [2], and Niederreiter and

2000 *Mathematics Subject Classification*: 11K38, 11K45, 94B05.

Research partially supported by the Austrian Science Fund (FWF) under the project S8306-MAT.

Xing [10]; see also the references in Section 6 of the last paper. We show that the concept of duality for linear codes can be applied to digital nets and that this leads to a new approach to various fundamental issues concerning digital nets. We use [3] as the basic reference for coding theory.

In Section 2 we recall the notion of the dual space (or, what amounts to the same thing, of the dual linear code) and we introduce concepts of weight and minimum distance that are appropriate for digital nets. In Section 3 we apply duality theory to the determination of the quality parameter for digital nets and to the analysis of the distribution of the points of digital nets in small intervals. In the last section we show that the tools of duality theory can lead to new construction principles for digital nets.

2. Dual space and minimum distance. Let s and m be positive integers and let $\mathbb{F}_b$ be the finite field of prime-power order b. Let $\mathcal{N}$ be an arbitrary linear subspace of $\mathbb{F}_b^{sm}$. Let H be a matrix over $\mathbb{F}_b$ with sm columns such that the row space of H is equal to $\mathcal{N}$. Define the *dual space* $\mathcal{N}^\perp \subseteq \mathbb{F}_b^{sm}$ of $\mathcal{N}$ to be the null space of H. It is easy to see that $\mathcal{N}^\perp$ depends only on $\mathcal{N}$ and not on the specific choice of H. Also

$$\dim(\mathcal{N}^\perp) = sm - \dim(\mathcal{N}) \tag{1}$$

and $(\mathcal{N}^\perp)^\perp = \mathcal{N}$.

Let G be a matrix over $\mathbb{F}_b$ with sm columns such that the row space of G is equal to $\mathcal{N}^\perp$. Then

$$HG^\top = 0.$$

This is an analog of the relationship between a generator matrix and a parity-check matrix of a linear code.

For $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}_b^m$ we introduce the weight $v(\mathbf{a})$ by $v(\mathbf{a}) = 0$ if $\mathbf{a} = \mathbf{0}$, $v(\mathbf{a}) = \max\{j : a_j \neq 0\}$ if $\mathbf{a} \neq \mathbf{0}$. We extend this definition to $\mathbb{F}_b^{sm}$ by writing a vector $\mathbf{A} \in \mathbb{F}_b^{sm}$ as the concatenation of s vectors of length m, i.e.,

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

and putting

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

Remark 2. In the case $m = 1$ the weight V_m reduces to the classical Hamming weight of a vector. If we define the distance $d_m(\mathbf{A}, \mathbf{B})$ of $\mathbf{A}, \mathbf{B} \in \mathbb{F}_b^{sm}$ by $d_m(\mathbf{A}, \mathbf{B}) = V_m(\mathbf{A} - \mathbf{B})$, then $\mathbb{F}_b^{sm}$ turns into a metric space, which for $m = 1$ is the Hamming space. In the context of low-discrepancy point sets and pseudorandom numbers, the weight V_m was first used by Niederreiter [4], [6]; see also Skriganov [11] for a recent application.

Definition 2. For any nonzero linear subspace $\mathcal{N}$ of $\mathbb{F}_b^{sm}$ we define the *minimum distance*

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

Furthermore, we put $\delta_m(\{\mathbf{0}\}) = sm + 1$.

It is trivial that $\delta_m(\mathcal{N}) \geq 1$ for any linear subspace $\mathcal{N}$ of $\mathbb{F}_b^{sm}$. The following is a generalization of the Singleton bound in coding theory. The Singleton bound corresponds to the case $m = 1$.

Proposition 1. *For any linear subspace $\mathcal{N}$ of $\mathbb{F}_b^{sm}$ we have*

$$\delta_m(\mathcal{N}) \leq sm - \dim(\mathcal{N}) + 1.$$

Proof. Put $h = \dim(\mathcal{N})$ and note that the result is trivial for $h = 0$. For $h \geq 1$ let $\pi : \mathcal{N} \to \mathbb{F}_b^h$ be the linear transformation which maps $\mathbf{A} \in \mathcal{N}$ to the h-tuple of the last h coordinates of $\mathbf{A}$. If π is surjective, then there exists a nonzero $\mathbf{A}_1 \in \mathcal{N}$ with

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

Then

$$V_m(\mathbf{A}_1) \leq sm - h + 1.$$

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

$$V_m(\mathbf{A}_2) \leq sm - h.$$

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

Definition 3. Let k, m, s be positive integers and let d be an integer with $0 \leq d \leq \min(k, sm)$. The system $\{\mathbf{c}_j^{(i)} \in \mathbb{F}_b^k : 1 \leq j \leq m,\ 1 \leq i \leq s\}$ is called a *(d, k, m, s)-system over* $\mathbb{F}_b$ if for any integers $d_1, \ldots, d_s$ with $0 \leq d_i \leq m$ for $1 \leq i \leq s$ and $\sum_{i=1}^{s} d_i = d$ the system $\{\mathbf{c}_j^{(i)} \in \mathbb{F}_b^k : 1 \leq j \leq d_i,\ 1 \leq i \leq s\}$ is linearly independent over $\mathbb{F}_b$ (the empty system is considered linearly independent). A (d, m, m, s)-system over $\mathbb{F}_b$ is also called a *(d, m, s)-system over* $\mathbb{F}_b$.

For a given system $\{\mathbf{c}_j^{(i)} \in \mathbb{F}_b^k : 1 \leq j \leq m,\ 1 \leq i \leq s\}$ let C_i, $1 \leq i \leq s$, be the $k \times m$ matrix with the column vectors $\mathbf{c}_1^{(i)}, \ldots, \mathbf{c}_m^{(i)}$. Combine these matrices into the matrix

$$C = (C_1 | C_2 | \ldots | C_s) \in \mathbb{F}_b^{k \times sm},$$

so that $C_1, \ldots, C_s$ are submatrices of C. Let $\mathcal{C}$ be the row space of C.

Theorem 1. *The system $\{\mathbf{c}_j^{(i)} \in \mathbb{F}_b^k : 1 \leq j \leq m,\ 1 \leq i \leq s\}$ is a (d, k, m, s)-system over $\mathbb{F}_b$ if and only if the dual space $\mathcal{C}^{\perp}$ of the row space $\mathcal{C}$ satisfies $\delta_m(\mathcal{C}^{\perp}) \geq d + 1$.*

Proof. The result is trivial if $\mathcal{C} = \mathbb{F}_b^{sm}$. So we can assume that $\mathcal{C}$ is a proper subspace of $\mathbb{F}_b^{sm}$. For $\mathbf{A} = (\mathbf{a}^{(1)}, \dots, \mathbf{a}^{(s)})^\top \in \mathbb{F}_b^{sm}$ with

$$\mathbf{a}^{(i)} = (a_1^{(i)}, \dots, a_m^{(i)}) \in \mathbb{F}_b^m \quad \text{for } 1 \le i \le s$$

we have

$$\sum_{i=1}^{s} \sum_{j=1}^{m} a_j^{(i)} \mathbf{c}_j^{(i)} = \mathbf{0} \in \mathbb{F}_b^k$$

if and only if

$$C\,\mathbf{A} = \mathbf{0} \in \mathbb{F}_b^k,$$

i.e., if and only if $\mathbf{A} \in \mathcal{C}^\perp$.

Now let the given system be a (d,k,m,s)-system over $\mathbb{F}_b$ and consider any nonzero $\mathbf{A} \in \mathcal{C}^\perp$. Then from the above we get

$$\sum_{i=1}^{s} \sum_{j=1}^{m} a_j^{(i)} \mathbf{c}_j^{(i)} = \mathbf{0} \in \mathbb{F}_b^k.$$

Put $v(\mathbf{a}^{(i)}) = v_i$ for $1 \le i \le s$, then

$$\sum_{i=1}^{s} \sum_{j=1}^{v_i} a_j^{(i)} \mathbf{c}_j^{(i)} = \mathbf{0} \in \mathbb{F}_b^k.$$

Since not all coefficients in this linear relation are 0, the system $\{\mathbf{c}_j^{(i)} \in \mathbb{F}_b^k : 1 \le j \le v_i, 1 \le i \le s\}$ is linearly dependent over $\mathbb{F}_b$. Thus, the definition of a (d,k,m,s)-system over $\mathbb{F}_b$ implies that $\sum_{i=1}^{s} v_i \ge d+1$. Therefore

$$V_m(\mathbf{A}) = \sum_{i=1}^{s} v(\mathbf{a}^{(i)}) = \sum_{i=1}^{s} v_i \ge d+1,$$

and so $\delta_m(\mathcal{C}^\perp) \ge d+1$.

Conversely, assume that $\delta_m(\mathcal{C}^\perp) \ge d+1$. We have to show that any system $\{\mathbf{c}_j^{(i)} \in \mathbb{F}_b^k : 1 \le j \le d_i, 1 \le i \le s\}$ with $0 \le d_i \le m$ for $1 \le i \le s$ and $\sum_{i=1}^{s} d_i = d$ is linearly independent over $\mathbb{F}_b$. Suppose, on the contrary, that such a system were linearly dependent over $\mathbb{F}_b$, i.e., that there exist coefficients $a_j^{(i)} \in \mathbb{F}_b$, not all 0, such that

$$\sum_{i=1}^{s} \sum_{j=1}^{d_i} a_j^{(i)} \mathbf{c}_j^{(i)} = \mathbf{0} \in \mathbb{F}_b^k.$$

Define $a_j^{(i)} = 0$ for $d_i < j \le m, 1 \le i \le s$, then

$$\sum_{i=1}^{s} \sum_{j=1}^{m} a_j^{(i)} \mathbf{c}_j^{(i)} = \mathbf{0} \in \mathbb{F}_b^k.$$

By what we have shown at the beginning of the proof, we get $\mathbf{A} \in \mathcal{C}^{\perp}$, and so $V_m(\mathbf{A}) \geq d+1$. On the other hand, $v(\mathbf{a}^{(i)}) \leq d_i$ for $1 \leq i \leq s$, and so

$$V_m(\mathbf{A}) = \sum_{i=1}^{s} v(\mathbf{a}^{(i)}) \leq \sum_{i=1}^{s} d_i = d,$$

which is a contradiction. ■

3. Digital nets. We consider digital (t,m,s)-nets constructed over the finite field $\mathbb{F}_b$. Such a digital net is determined by a system $\{\mathbf{c}_j^{(i)} \in \mathbb{F}_b^m : 1 \leq j \leq m, 1 \leq i \leq s\}$ of vectors, where m and s are positive integers. For $1 \leq i \leq s$ let C_i be the $m \times m$ matrix with column vectors $\mathbf{c}_1^{(i)}, \ldots, \mathbf{c}_m^{(i)}$. The matrices $C_1, \ldots, C_s$ are called the *generating matrices* of the digital net.

The points $\mathbf{x}_0, \ldots, \mathbf{x}_{b^m-1}$ of the digital net are constructed in the following way. In order to obtain the nth point $\mathbf{x}_n$, consider the b-ary expansion of n, given by $n = \sum_{j=1}^{m} a_j(n) b^{j-1}$. Choosing fixed bijections $a_j \mapsto \overline{a_j}$ from $Z_b := \{0,1,\ldots,b-1\}$ to $\mathbb{F}_b$ for each $j, 1 \leq j \leq m$, we identify n with the row vector

$$\mathbf{n} = (\overline{a_1(n)}, \ldots, \overline{a_m(n)}) \in \mathbb{F}_b^m.$$

Then, using fixed bijections $\overline{x_{n,j}^{(i)}} \mapsto x_{n,j}^{(i)}$ from $\mathbb{F}_b$ to Z_b for each $i, j, 1 \leq i \leq s$, $1 \leq j \leq m$, we map the vectors

$$(\overline{x_{n,1}^{(i)}}, \ldots, \overline{x_{n,m}^{(i)}}) := \mathbf{n} C_i \in \mathbb{F}_b^m$$

to the real numbers

$$x_n^{(i)} = \sum_{j=1}^{m} x_{n,j}^{(i)} b^{-j}$$

to obtain the point

$$\mathbf{x}_n = (x_n^{(1)}, \ldots, x_n^{(s)}) \in [0,1)^s.$$

Definition 4. If the point set $\mathcal{P} = \{\mathbf{x}_0, \ldots, \mathbf{x}_{b^m-1}\}$ constructed above forms a (strict) (t,m,s)-net in base b, then we call $\mathcal{P}$ a *digital* (*strict*) (t,m,s)*-net constructed over* $\mathbb{F}_b$.

We set up the *overall generating matrix*

$$C = (C_1|C_2|\ldots|C_s) \in \mathbb{F}_b^{m \times sm}$$

of the digital net and let $\mathcal{C}$ be its row space. We call $\mathcal{C}$ a *row space* of the digital net.

Theorem 2. *Let* $0 \leq t \leq m$. *Then the system* $\{\mathbf{c}_j^{(i)} \in \mathbb{F}_b^m : 1 \leq j \leq m$, $1 \leq i \leq s\}$ *generates a digital* (t,m,s)*-net constructed over* $\mathbb{F}_b$ *if and only if* $\delta_m(\mathcal{C}^{\perp}) \geq m-t+1$.

Proof. We know that the given system generates a digital (t,m,s)-net constructed over $\mathbb{F}_b$ if and only if it is an $(m-t,m,s)$-system over $\mathbb{F}_b$ (see e.g. [10, Lemma 3]). The rest follows from Theorem 1. ∎

Corollary 1. *The system* $\{\mathbf{c}_j^{(i)} \in \mathbb{F}_b^m : 1 \le j \le m,\ 1 \le i \le s\}$ *generates a digital strict* (t,m,s)*-net constructed over* $\mathbb{F}_b$ *with* $t = m - \delta_m(\mathcal{C}^\perp) + 1$.

Proof. By Theorem 2 we have $t \ge m - \delta_m(\mathcal{C}^\perp) + 1$. Also $\dim(\mathcal{C}) \le m$, and so $\dim(\mathcal{C}^\perp) \ge sm - m$ by (1). Thus, $\delta_m(\mathcal{C}^\perp) \le m+1$ by Proposition 1, and so $m - \delta_m(\mathcal{C}^\perp) + 1$ lies in the interval $[0,m]$. Hence $m - \delta_m(\mathcal{C}^\perp) + 1$ is a possible value of t. ∎

A further application of dual spaces for digital (t,m,s)-nets is the counting of points of a net $\mathcal{P}$ in a ("small") b-ary box J. This problem is of interest, e.g., in the investigation of integration error variation (see [9]).

Theorem 3. *Let a digital* (t,m,s)*-net* $\mathcal{P}$ *constructed over* $\mathbb{F}_b$ *and a* b*-ary box*

$$J = \prod_{i=1}^{s} [n_i/b^{d_i}, (n_i+1)/b^{d_i}) \subseteq [0,1)^s, \qquad d_i, n_i \in \mathbb{Z}, 0 \le d_i \le m, 1 \le i \le s,$$

be given. The maximum number of points of $\mathcal{P}$ *in* J *for any choice of* $0 \le n_i < b^{d_i}, 1 \le i \le s$, *is*

$$b^{m-(d_1+\ldots+d_s)} |\mathcal{L}(\mathbf{d})|,$$

where $\mathbf{d} = (d_1, \ldots, d_s)$ *and*

$$\mathcal{L}(\mathbf{d}) := \{(\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(s)}) \in \mathcal{C}^\perp : v(\mathbf{a}^{(i)}) \le d_i \text{ for } 1 \le i \le s\}.$$

Proof. Let $d = \sum_{i=1}^{s} d_i$. We know by [9, Theorem 3.2] that the maximum number of points of $\mathcal{P}$ in J is $b^{m-\operatorname{rank}(C_{\mathbf{d}})}$, where

$$C_{\mathbf{d}} = (\mathbf{c}_1^{(1)} \ldots \mathbf{c}_{d_1}^{(1)} \ldots \mathbf{c}_1^{(s)} \ldots \mathbf{c}_{d_s}^{(s)}) \in \mathbb{F}_b^{m \times d}.$$

Consider the system of linear equations $C_{\mathbf{d}} \widehat{\mathbf{A}} = \mathbf{0} \in \mathbb{F}_b^m$, $\widehat{\mathbf{A}} \in \mathbb{F}_b^d$. The solution space $\mathcal{S}$ of this system is of dimension $d - \operatorname{rank}(C_{\mathbf{d}})$. For any

$$\widehat{\mathbf{A}} = (a_1^{(1)}, \ldots, a_{d_1}^{(1)}, \ldots, a_1^{(s)}, \ldots, a_{d_s}^{(s)})^\top \in \mathcal{S}$$

build the vector

$$\mathbf{A} = (\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(s)})^\top = (a_1^{(1)}, \ldots, a_m^{(1)}, \ldots, a_1^{(s)}, \ldots, a_m^{(s)})^\top \in \mathbb{F}_b^{sm}$$

by setting $a_{d_i+1}^{(i)} = \ldots = a_m^{(i)} = 0$ for all $1 \le i \le s$. Then $v(\mathbf{a}^{(i)}) \le d_i$ for $1 \le i \le s$ and $C\mathbf{A} = \mathbf{0} \in \mathbb{F}_b^m$, so $\mathbf{A} \in \mathcal{L}(\mathbf{d})$.

On the other hand, for any vector $\mathbf{A} \in \mathcal{L}(\mathbf{d})$ the vector $\widehat{\mathbf{A}} \in \mathbb{F}_b^d$ obtained by omitting the entries $a_{d_i+1}^{(i)}, \ldots, a_m^{(i)}$, $1 \le i \le s$, is a solution to $C_{\mathbf{d}} \widehat{\mathbf{A}} = \mathbf{0}$ and therefore in $\mathcal{S}$.

So $|\mathcal{S}| = |\mathcal{L}(\mathbf{d})|$ and

$$b^{m-d}|\mathcal{L}(\mathbf{d})| = b^{m-d}|\mathcal{S}| = b^{m-\mathrm{rank}(C_{\mathbf{d}})}$$

is the maximum number of points of $\mathcal{P}$ in J. ■

Note that by the definition of a (t, m, s)-net in base b, the number of points of $\mathcal{P}$ in J is exactly $b^{m-(d_1+\ldots+d_s)}$ for $d_1 + \ldots + d_s \le m - t$, so the size of $\mathcal{L}(\mathbf{d})$ is indicative of the excess of points in smaller intervals.

The vector spaces $\mathcal{L}(\mathbf{d})$ may also be used for the characterization of (d, k, m, s)-systems.

Theorem 4. *The system* $\{\mathbf{c}_j^{(i)} \in \mathbb{F}_b^k : 1 \le j \le m, 1 \le i \le s\}$ *is a* (d, k, m, s)*-system over* $\mathbb{F}_b$ *if and only if* $\dim(\mathcal{L}(\mathbf{d})) = 0$ *for all* $\mathbf{d} = (d_1, \ldots, d_s) \in \{0, 1, \ldots, m\}^s$ *with* $d_1 + \ldots + d_s = d$.

Proof. We show that the condition is equivalent to $\delta_m(\mathcal{C}^\perp) \ge d + 1$, so that the result follows from Theorem 1.

If $d \le \delta_m(\mathcal{C}^\perp) - 1$, then for any $\mathbf{d} = (d_1, \ldots, d_s) \in \{0, 1, \ldots, m\}^s$ with $d_1 + \ldots + d_s = d$ and any vector $\mathbf{A} = (\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(s)}) \in \mathcal{C}^\perp \setminus \{\mathbf{0}\}$ we have $V_m(\mathbf{A}) \ge d+1$, therefore for at least one i we have $v(\mathbf{a}^{(i)}) > d_i$, so $\mathbf{A} \notin \mathcal{L}(\mathbf{d})$ and $\dim(\mathcal{L}(\mathbf{d})) = \dim(\{\mathbf{0}\}) = 0$.

On the other hand, suppose that $\mathcal{L}(\mathbf{d}) = \{\mathbf{0}\}$ for all $\mathbf{d}$ as in the theorem. If we had $\delta_m(\mathcal{C}^\perp) \le d$, then there exists a vector $\mathbf{A} = (\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(s)}) \in \mathcal{C}^\perp \setminus \{\mathbf{0}\}$ with $V_m(\mathbf{A}) \le d$. Put $v(\mathbf{a}^{(i)}) = e_i$ for $1 \le i \le s$, then $\sum_{i=1}^s e_i \le d$. Choose integers $d_1, \ldots, d_s$ with $e_i \le d_i \le m$ for $1 \le i \le s$ and $\sum_{i=1}^s d_i = d$. With $\mathbf{d}_0 = (d_1, \ldots, d_s)$ we get $\mathbf{A} \in \mathcal{L}(\mathbf{d}_0)$, which is a contradiction. ■

4. An application to the construction of digital nets.

We show that duality theory leads to new construction principles for digital nets. We start from a digital (t_1, m, s)-net and a digital (t_2, m, s)-net constructed over $\mathbb{F}_b$ and let $\mathcal{C}_1 \subseteq \mathbb{F}_b^{sm}$ and $\mathcal{C}_2 \subseteq \mathbb{F}_b^{sm}$ be corresponding row spaces. Let $\mathcal{C}_1^\perp \subseteq \mathbb{F}_b^{sm}$ and $\mathcal{C}_2^\perp \subseteq \mathbb{F}_b^{sm}$ be the dual spaces of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. We have

$$\dim(\mathcal{C}_1^\perp) \ge (s-1)m, \quad \dim(\mathcal{C}_2^\perp) \ge (s-1)m.$$

The following method of obtaining a digital $(t, 2m, s)$-net constructed over $\mathbb{F}_b$ may be viewed as an analog of a construction in coding theory (see [3, Section 2.9]). We first construct a linear subspace $\mathcal{N}$ of $\mathbb{F}_b^{2sm}$ by certain concatenations of vectors. Let

$$\mathbf{A} = (\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(s)}) \in \mathcal{C}_1^\perp, \quad \mathbf{a}^{(i)} \in \mathbb{F}_b^m \quad \text{for } 1 \le i \le s,$$
$$\mathbf{B} = (\mathbf{b}^{(1)}, \ldots, \mathbf{b}^{(s)}) \in \mathcal{C}_2^\perp, \quad \mathbf{b}^{(i)} \in \mathbb{F}_b^m \quad \text{for } 1 \le i \le s,$$

be the generic vectors of $\mathcal{C}_1^\perp$ and $\mathcal{C}_2^\perp$, respectively. Then the generic vector of $\mathcal{N}$ is

$$\mathbf{N} = (\mathbf{a}^{(1)}, \mathbf{a}^{(1)} + \mathbf{b}^{(1)}, \ldots, \mathbf{a}^{(s)}, \mathbf{a}^{(s)} + \mathbf{b}^{(s)}) \in \mathbb{F}_b^{2sm}.$$

We have

$$\dim(\mathcal{N}) = \dim(\mathcal{C}_1^\perp) + \dim(\mathcal{C}_2^\perp) \geq 2(s-1)m,$$

and so

$$\dim(\mathcal{N}^\perp) = 2sm - \dim(\mathcal{N}) \leq 2m$$

by (1). Put $\mathcal{C} = \mathcal{N}^\perp \subseteq \mathbb{F}_b^{2sm}$ and let the matrix $C \in \mathbb{F}_b^{2m\times 2sm}$ be such that its row space is $\mathcal{C}$. Then C is the overall generating matrix of a digital $(t, 2m, s)$-net $\mathcal{P}$ constructed over $\mathbb{F}_b$ and $\mathcal{C}$ is a row space of $\mathcal{P}$ (see the beginning of Section 3).

In order to bound the quality parameter t for the net $\mathcal{P}$, we define $(x)_+ = \max(x, 0)$ for real x and

$$D(\mathcal{C}_1^\perp, \mathcal{C}_2^\perp) = \max_{1\leq i\leq s} \max_{R_i} (v(\mathbf{a}^{(i)}) - v(\mathbf{a}^{(i)} + \mathbf{b}^{(i)}))_+,$$

where R_i is the set of all ordered pairs $(\mathbf{A}, \mathbf{B})$ with $\mathbf{A} = (\mathbf{a}^{(1)}, \dots, \mathbf{a}^{(s)}) \in \mathcal{C}_1^\perp \setminus \{\mathbf{0}\}$, $\mathbf{B} = (\mathbf{b}^{(1)}, \dots, \mathbf{b}^{(s)}) \in \mathcal{C}_2^\perp \setminus \{\mathbf{0}\}$, $\mathbf{a}^{(k)} + \mathbf{b}^{(k)} = \mathbf{0}$ for $k \neq i$ and $\mathbf{a}^{(i)} + \mathbf{b}^{(i)} \neq \mathbf{0}$. The maximum over R_i is defined to be 0 if R_i is empty. Note that we have $0 \leq D(\mathcal{C}_1^\perp, \mathcal{C}_2^\perp) \leq m - 1$.

Theorem 5. *The point set $\mathcal{P}$ defined above is a digital $(t, 2m, s)$-net constructed over $\mathbb{F}_b$ with*

$$t \leq \max(t_1 + D(\mathcal{C}_1^\perp, \mathcal{C}_2^\perp), t_2)$$

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

$$t \leq \max(t_1 + D(\mathcal{C}_1^\perp, \mathcal{C}_2^\perp), t_2, 2m + 1 - \delta_m(\mathcal{C}_1^\perp \cap \mathcal{C}_2^\perp))$$

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

Proof. By Corollary 1, $\mathcal{P}$ is a digital strict $(t, 2m, s)$-net constructed over $\mathbb{F}_b$ with

$$t = 2m - \delta_{2m}(\mathcal{N}) + 1. \tag{2}$$

Thus, we have to find a lower bound for $\delta_{2m}(\mathcal{N})$, and so for $V_{2m}(\mathbf{N})$ for all nonzero $\mathbf{N} \in \mathcal{N}$. By the construction we have

$$V_{2m}(\mathbf{N}) = \sum_{i=1}^{s} v(\mathbf{a}^{(i)}, \mathbf{a}^{(i)} + \mathbf{b}^{(i)}).$$

We now distinguish several cases. If $\mathbf{A} = \mathbf{0}$, then $\mathbf{B} \neq \mathbf{0}$ and

$$V_{2m}(\mathbf{N}) = \sum_{\substack{i=1 \\ \mathbf{b}^{(i)}\neq\mathbf{0}}}^{s} (m + v(\mathbf{b}^{(i)})) \geq m + V_m(\mathbf{B}) \geq 2m - t_2 + 1,$$

where we used that $\delta_m(\mathcal{C}_2^\perp) \geq m - t_2 + 1$ by Theorem 2. If $\mathbf{B} = \mathbf{0}$, then $\mathbf{A} \neq \mathbf{0}$ and analogously

$$V_{2m}(\mathbf{N}) \geq 2m - t_1 + 1.$$

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

$$V_{2m}(\mathbf{N}) = V_m(\mathbf{A}) \geq \delta_m(\mathcal{C}_1^{\perp} \cap \mathcal{C}_2^{\perp}).$$

Finally, if $\mathbf{A} \neq \mathbf{0}$, $\mathbf{B} \neq \mathbf{0}$, and $\mathbf{A} + \mathbf{B} \neq \mathbf{0}$, then

$$V_{2m}(\mathbf{N}) = \sum_{\substack{i=1 \\ \mathbf{a}^{(i)}+\mathbf{b}^{(i)} \neq \mathbf{0}}}^{s} (m + v(\mathbf{a}^{(i)} + \mathbf{b}^{(i)})) + \sum_{\substack{i=1 \\ \mathbf{a}^{(i)}+\mathbf{b}^{(i)} = \mathbf{0}}}^{s} v(\mathbf{a}^{(i)}).$$

If the first sum in the last expression has at least two terms, then $V_{2m}(\mathbf{N}) \geq 2m + 2$. Otherwise, it has exactly one term, say for $i = i_0$, and then

$$\begin{aligned} V_{2m}(\mathbf{N}) &= m + v(\mathbf{a}^{(i_0)} + \mathbf{b}^{(i_0)}) + \sum_{i=1,\, i \neq i_0}^{s} v(\mathbf{a}^{(i)}) \\ &= m + V_m(\mathbf{A}) + v(\mathbf{a}^{(i_0)} + \mathbf{b}^{(i_0)}) - v(\mathbf{a}^{(i_0)}) \\ &\geq 2m - t_1 + 1 - (v(\mathbf{a}^{(i_0)}) - v(\mathbf{a}^{(i_0)} + \mathbf{b}^{(i_0)}))_+ \\ &\geq 2m - t_1 + 1 - D(\mathcal{C}_1^{\perp}, \mathcal{C}_2^{\perp}). \end{aligned}$$

Altogether, this yields

$$\delta_{2m}(\mathcal{N}) \geq \min(2m - t_1 + 1 - D(\mathcal{C}_1^{\perp}, \mathcal{C}_2^{\perp}), 2m - t_2 + 1)$$

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

$$\delta_{2m}(\mathcal{N}) \geq \min(2m - t_1 + 1 - D(\mathcal{C}_1^{\perp}, \mathcal{C}_2^{\perp}), 2m - t_2 + 1, \delta_m(\mathcal{C}_1^{\perp} \cap \mathcal{C}_2^{\perp}))$$

if $\mathcal{C}_1^{\perp} \cap \mathcal{C}_2^{\perp} \neq \{\mathbf{0}\}$, and thus the result of the theorem in view of (2). ■

Theorem 5 should just serve as an illustration of the new construction principles for digital nets that we believe are possible with the duality method. The extensively developed theory of linear codes can be used as a source of analogies that may lead to further construction principles for digital nets on the basis of duality.

References

[1] M. J. Adams and B. L. Shader, *A construction for (t, m, s)-nets in base q*, SIAM J. Discrete Math. 10 (1997), 460–468.

[2] K. M. Lawrence, A. Mahalanabis, G. L. Mullen and W. Ch. Schmid, *Construction of digital (t, m, s)-nets from linear codes*, in: Finite Fields and Applications, S. Cohen and H. Niederreiter (eds.), London Math. Soc. Lecture Note Series 233, Cambridge Univ. Press, Cambridge, 1996, 189–208.

[3] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

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

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

[6] —, *A statistical analysis of generalized feedback shift register pseudorandom number generators*, SIAM J. Sci. Statist. Comput. 8 (1987), 1035–1051.

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

[8] —, *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.

[9] H. Niederreiter and G. Pirsic, *The microstructure of* (t, m, s)*-nets*, J. Complexity, to appear.

[10] H. Niederreiter and C. P. Xing, *Nets*, (t, s)*-sequences, and algebraic geometry*, in: Random and Quasi-Random Point Sets, P. Hellekalek and G. Larcher (eds.), Lecture Notes in Statist. 138, Springer, New York, 1998, 267–302.

[11] M. M. Skriganov, *Coding theory and uniform distributions*, preprint, Steklov Math. Institute, St. Petersburg, 1999.

Institute of Discrete Mathematics
Austrian Academy of Sciences
Sonnenfelsgasse 19
A-1010 Wien, Austria
E-mail: niederreiter@oeaw.ac.at
gottlieb.pirsic@oeaw.ac.at

Received on 24.3.2000 (3786)