Coding-theoretic constructions for (t, m, s)-nets and ordered orthogonal arrays

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA),

Yves Edel
Mathematisches Institut der Universität
Im Neuenheimer Feld 288
69120 Heidelberg (Germany), and

Wolfgang Ch. Schmid*
Institut für Mathematik
Universität Salzburg
Salzburg (Austria)

April 8, 2002

1 Introduction

$(t, m, s)-$nets were defined by Niederreiter [17] in the context of quasi-Monte Carlo methods of numerical integration. Niederreiter pointed out close connections to certain combinatorial and algebraic structures. This was made precise in the work of Lawrence, Mullen and Schmid [11, 15, 24]. These

*Research partially supported by the Austrian Science Fund (FWF) Grant S8311-MAT.

authors introduce a large class of finite combinatorial structures, which we will call **ordered orthogonal arrays** OOA. These OOA contain orthogonal arrays as a subclass. $(t, m, s)_q$-nets (that is, (t, m, s)-nets in base q as in the original Definition 2.2 in [17]) are equivalent to another parametric subclass of OOA. Loosely speaking a $(t, m, s)_q$-net is **linear** if it is defined over the field $\mathbb{F}_q$ with q elements. The duality between linear codes and linear orthogonal arrays carries over to the more general setting of linear OOA (see [14] or [20]). Here OOA generalize orthogonal arrays (dual codes). The weight function generalizing Hamming weight was first described by Niederreiter in [16, 18]. It was systematically exploited by Rosenbloom-Tsfasman in [23]. We use the term NRT-space for the corresponding metric space. A description is in Section 2.

Our main results are generalizations of coding-theoretic construction techniques from Hamming space to NRT-space, most notably concatenation (equivalently: Kronecker products), the $(u, u + v)$-construction and the Gilbert-Varshamov bound.

Let $k = m-t$ denote the **strength** of a net. If a linear $(t, m, s)_q$-net exists, where $m < s$, then a linear code $[s, s - m, k + 1]_q$ exists. From this point of view it is a basic problem (the problem of net-embeddability) to decide when a code $[s, s-m, k+1]_q$ can be completed to a linear $(m-k, m, s)_q$-net. More generally we ask when a linear OOA with certain parameters can be embedded in a larger OOA. We speak of a theorem of Gilbert-Varshamov type if the existence of the larger OOA can be guaranteed whenever the parameters satisfy a certain numerical condition. In the final section we apply our theoretical construction techniques as well as computer-generated net embeddings of error-correcting codes to improve upon net-parameters for nets of moderate strength and dimension defined over small fields.

2 Linear nets and linear ordered orthogonal arrays

A (t, m, s)-net is a subset of Euclidean $s-$space. We mentioned in the introduction that (t, m, s)-nets can equivalently be described by finite geometrical objects. More precisely (t, m, s)-nets are equivalent to a subclass of **ordered orthogonal arrays.** For our purposes this description is more natural. We use it as a definition. Moreover we concentrate on the linear case.

Definition 1. *Let $\Omega = \Omega^{(T,s)}$ be a set of Ts elements, partitioned into s* **blocks** *$B_i, i = 1, 2 \ldots, s$, where $B_i = \{\omega_1^{(i)}, \ldots, \omega_T^{(i)}\}$. Each block carries a total ordering:*

$$\omega_1^{(i)} < \omega_2^{(i)} < \cdots < \omega_T^{(i)}.$$

This gives Ω the structure of a partially ordered set, the union of s totally ordered sets of T points each. We consider Ω as a basis of a $Ts-$dimensional vector space $\mathbb{F}_q^{(T,s)}$. An **ideal** *in Ω is a set of elements closed under predecessors. An* **antiideal** *is a subset closed under followers. Observe that antiideals are precisely the complements of ideals.*

We visualize elements $x = (x_j^{(i)}) \in \mathbb{F}_q^{(T,s)}, i = 1, \ldots, s; j = 1, \ldots, T$ either as strings of length Ts, divided in s segments (the blocks) of length T each, or as matrices with T rows and s columns. Refer to these representations as **vector notation** and **matrix notation,** respectively. The interpretation of $x \in \mathbb{F}_q^{(T,s)}$ as a point in the $s-$dimensional unit cube is obtained by reading the $x_j^{(i)}$ for fixed i as the T first digits of the $q-$ary expansion of a real number between 0 and 1. As an example, the point $\begin{array}{|c|c|c|c|}\hline 0&0&1&1\\ \hline 1&1&1&0\\ \hline 1&0&0&1\\ \hline\end{array}$ in $\mathbb{F}_2^{(3,4)}$ is mapped to the point $(\frac{3}{8}, \frac{1}{4}, \frac{3}{4}, \frac{5}{8}) \in [0,1)^4$. This also motivates the hierarchical ordering inside the blocks.

We introduce some more terminology, which will be helpful in describing the basic parameters of NRT-space.

Definition 2. *We refer to coordinate positions of $\mathbb{F}_q^{(T,s)}$ as* **cells.** *They are in obvious bijection with the elements of Ω. The* **breadth** *$b = b(x)$ of a vector $x \in \mathbb{F}_q^{(T,s)}$ is the number of blocks $B_i, i = 1, 2, \ldots, s$ where x has a nonzero entry. The ideal $K = K(x)$ generated by x is the smallest ideal containing the support of x. The breadth of an ideal K is the number of blocks it intersects nontrivially. Let $n = |K|$ be the* **size** *of K. The* **type** *$\pi = \pi(K)$ is the partition n, where the multiplicity f_i of i as a part of π is the number of blocks, which intersect K in i points. The breadth $b(\pi)$ of a partition is the number of its nonzero parts. If $\pi = \pi(K(x))$, then $b(\pi) = b(x)$.*

Definition 3 (NRT-metric). *Let $x \in \mathbb{F}_q^{(T,s)}$. The* **weight** *of x is*

$$\rho(x) = \rho(x, 0) = \sum_{i=1}^{s} T - \max\{j \mid x_1^{(i)} = \ldots x_j^{(i)} = 0\}$$

The **distance** $\rho(x,y)$ *is defined as* $\rho(x,y)=\rho(x-y)$. *The* **minimum weight** *(=minimum distance) of a subspace* $\mathcal{C}\subseteq \mathbb{F}_q^{(T,s)}$ *is the minimum among the weights of its nonzero members*

We may visualize the weight $\rho(x)$ as follows: in each block let the leading zeroes evaporate. The number of remaining cells is $\rho(x)$. It is clear that ρ is a metric. Also, $Ts-\rho(x,y)$ is the size of the maximal ideal on which x and y agree.

Definition 4. *Let* $S_l^{(T,s)}$ *be the number of vectors of weight* l *in* $\mathbb{F}_q^{(T,s)}$ *and* $V_l^{(T,s)}=\sum_{i=0}^l S_i^{(T,s)}$ *the volume of a ball of radius* l *in* $\mathbb{F}_q^{(T,s)}$.

Proposition 1. *We have*

$$S_l^{(T,s)}=\sum_{\pi}\binom{s}{f_T,\dots,f_1,s-b}(q-1)^b q^{l-b},$$

where the sum is over all partitions π *of* l *of depth* $\leq T$, *and* $b=b(\pi), f_i=f_i(\pi)$.

Proof. $S_l^{(T,s)}$ counts the vectors of $\mathbb{F}_q^{(T,s)}$, whose support generates an ideal of size l. The type of such an ideal K is a partition π as above. The number of vectors generating a fixed K of breadth b clearly is $(q-1)^b q^{l-b}$. It remains to count the ideals K with a given type π. This number is

$$\binom{s}{f_T}\binom{s-f_T}{f_{T-1}}\dots\binom{s-f_T-\dots-f_2}{f_1}=\binom{s}{f_T,\dots,f_1,s-b}.$$

■

We now define the objects we are primarily interested in.

Definition 5. *A linear subspace (code)* $\mathcal{C}\subseteq\mathbb{F}_q^{(T,s)}$ *has* **strength** $k=k(\mathcal{C})$ *if* k *is maximal such that the projection from* $\mathcal{C}$ *to any ideal of size* k *is surjective. We also call such a subspace an* **ordered orthogonal array** *OOA, which is* $q-$*linear, has* **length** s, **depth** T, **dimension** $m=\dim(\mathcal{C})$ *and strength* k.

A linear $(m-k,m,s)_q$-net is equivalent to an $m-$dimensional code $\mathcal{C}\subseteq\mathbb{F}_q^{(k,s)}$ of strength k. Observe also that linear OOA of depth 1 are precisely linear orthogonal arrays, in other words an $m-$dimensional code in $\mathbb{F}_q^{(1,s)}$ of strength k is the dual (with respect to the ordinary dot product) of a code $[s,s-m,k+1]_q$.

Definition 6. *Define a symmetric bilinear form on* $\mathbb{F}_q^{(T,s)}$ *by*

$$\langle x, y\rangle = \sum_{i=1}^{s} x_1^{(i)} y_T^{(i)} + x_2^{(i)} y_{T-1}^{(i)} + \cdots + x_T^{(i)} y_1^{(i)}.$$

The dual $\mathcal{C}^{\perp}$ *is defined with respect to this scalar product.*

Observe that $\mathbb{F}_q^{(1,s)}$ is the usual Hamming space, with its metric, the dot product and the corresponding notion of duality. Generalizing the notion of Hamming space we may call $\mathbb{F}_q^{(T,s)}$ with the NRT-metric and the corresponding notion of strength the **NRT-space.** It is an important albeit elementary observation that the duality (in Hamming space) between strength and minimum distance can be extended to our setting (see [14] or [20]).

Theorem 1. *Let* $\mathcal{C} \subseteq \mathbb{F}_q^{(T,s)}$ *be a linear subspace (code). Then*

$$\rho(\mathcal{C}^{\perp}) = k(\mathcal{C}) + 1.$$

We are led to the natural problem of generalizing coding-theoretic bounds and constructions from Hamming space to NRT-space.

3 Trace codes

Theorem 2. *Let* $\mathcal{C} \subseteq \mathbb{F}_{q^r}^{(T,s)}$ *of dimension* m *and strength* k*. We can construct* $\tilde{\mathcal{C}} \subseteq \mathbb{F}_q^{(T,rs)}$ *of dimension* rm *and strength* k*.*

Proof. Let $\{b_1, \ldots, b_r\}$ be a basis of $F = \mathbb{F}_{q^r} \mid \mathbb{F}_q$. We describe an $\mathbb{F}_q-$isomorphism $\tilde{}: \mathcal{C} \longrightarrow \tilde{\mathcal{C}}$ as follows: Let $tr : F \longrightarrow \mathbb{F}_q$ be the trace and $x \in \mathcal{C}$. The entry of $\tilde{x}$ in coordinate (i, a), where $1 \leq i \leq s, 1 \leq a \leq r$ and depth j is $\tilde{x}_j^{(i,a)} = tr(x_j^{(i)} b_a)$. It is obvious that we have an $\mathbb{F}_q-$ isomorphism as the kernel is trivial. In particular $\dim(\tilde{\mathcal{C}}) = mr$. It is also obvious that $\tilde{\mathcal{C}}$ still has strength k. ∎

The special case of nets was proved in [22].

4 Concatenation

The following construction may be seen as a concatenation construction or as a Kronecker product for linear codes in NRT-space. A different Kronecker product construction is in [21].

Theorem 3. *Let $\mathcal{C}_1 \subseteq \mathbb{F}_{q^r}^{(T_1,s_1)}$ of dimension m and $\mathcal{C}_2 \subseteq \mathbb{F}_q^{(T_2,s_2)}$ of dimension r. Let $\alpha : \mathbb{F}_{q^r} \longrightarrow \mathcal{C}_2$ be an $\mathbb{F}_q-$isomorphism. Define the concatenation $\mathcal{C}_2 \circ \mathcal{C}_1 = \alpha(\mathcal{C}_1) \subset \mathbb{F}_q^{(T_1T_2,s_1s_2)}$ as follows (in matrix notation): each $x \in \mathcal{C}_1$ yields $\alpha(x) \in \mathcal{C}_2 \circ \mathcal{C}_1$ by applying α to each entry of x. Then $\dim(\mathcal{C}_2 \circ \mathcal{C}_1) = mr$ and $k(\mathcal{C}_2 \circ \mathcal{C}_1) \geq \min\{k(\mathcal{C}_1), k(\mathcal{C}_2)\}$.*

Proof. As the elements of $\mathcal{C}_2 \circ \mathcal{C}_1$ are in bijection with those of $\mathcal{C}_1$, the statement concerning the dimension is obvious. Let $k = \min\{k(\mathcal{C}_1), k(\mathcal{C}_2)\}$. Consider an ideal K of size k in $\Omega^{(T_1T_2,s_1s_2)}$. The natural projection $\overline{K}$ to $\Omega^{(T_1,s_1)}$ is an ideal of size $\leq k$. We can therefore find $x \in \mathcal{C}_1$ such that $\alpha(x)$ has arbitrarily chosen entries from $\mathcal{C}_2$ in the positions of this ideal. For each $(i_1, j_1) \in \overline{K}$ the intersection of K with the corresponding $\Omega^{(T_2,s_2)}$ is itself an ideal, clearly of size $\leq k$. The claim follows. ■

The special cases of Theorem 3 when either $\mathcal{C}_1$ or $\mathcal{C}_2$ is a net and the other is an OA ($T_2 = 1$ or $T_1 = 1$) is in [22].

5 The $(u, u + v)$-construction

Theorem 4. *For $i = 1, 2$ let $\mathcal{C}_i \subset \mathbb{F}_q^{(T,s_i)}$ be linear OOA of dimension m_i and strength k_i, where $s_1 \leq s_2$. We can construct $\mathcal{C} \subset \mathbb{F}_q^{(T,s_1+s_2)}$ of dimension $m_1 + m_2$ and strength $\min\{k_2, 2k_1 + 1\}$.*

Proof. This is a direct generalization of the famous $(u, u + v)$-construction in coding theory, which seems to go back to [26]. Consider the duals $\mathcal{C}_i^\perp$. These have dimension $Ts_i - m_i$ and distance $k_i + 1$. We apply the $(u, u + v)$-construction to $\mathcal{C}_i^\perp$. Our $\mathcal{C}$ will be obtained by dualizing (back). More precisely let $C_i = (C_i^{(1)}, C_i^{(2)}, \ldots, C_i^{(s_i)})$ be a generic element of $\mathcal{C}_i, i = 1, 2$. We define $\mathcal{C}^\perp$ as the image of the $(u, u + v)$-mapping

$$u : \mathcal{C}_1^\perp \oplus \mathcal{C}_2^\perp \longrightarrow \mathbb{F}_q^{(T,s_1+s_2)}$$

given by

$$u(C_1, C_2) = (C_1^{(1)}, C_1^{(1)} + C_2^{(1)}, \ldots, C_1^{(s_1)}, C_1^{(s_1)} + C_2^{(s_1)}, C_2^{(s_1+1)}, \ldots, C_2^{(s_2)}).$$

It is obvious that u is $\mathbb{F}_q$-linear and injective. In particular $\dim(\mathcal{C}^\perp) = (Ts_1 - m_1) + (Ts_2 - m_2) = T(s_1 + s_2) - (m_1 + m_2)$, hence $\dim(\mathcal{C}) = m_1 + m_2$. In order to find the strength of $\mathcal{C}$ we have to determine the distance of $\mathcal{C}^\perp$.

Let $C_2 = 0, C_1 \neq 0$. Then $\rho(C_1, 0) = 2\rho(C_1) \geq 2(k_1 + 1)$. Let $C_2 \neq 0$. For each $j = 1, 2, \ldots, s_1$ the weight of the pair of columns $(C_1^{(j)}, C_1^{(j)} + C_2^{(j)})$ is at least the weight of the single column $C_2^{(j)}$. It follows $\rho(C_1, C_2) \geq k_2 + 1$ if $C_2 \neq 0$. ■

Let $k_2 = 2k_1 + 1$. In order to obtain a net as result, we must have $T = k_2$. This means that $\mathcal{C}_2$ is a $(t_2, m_2, s_2)_q$-net, $k_2 = m_2 - t_2$, whereas $\mathcal{C}_1$ has depth $T = k_2 > k_1$ and strength k_1. The effective depth of $\mathcal{C}_1$ is therefore k_1, and $\mathcal{C}_1$ is obtained from a net of strength k_1 by adding meaningless rows. We have seen the following:

Corollary 1. *Assume $k_2 \leq 2k_1 + 1$ and there exist linear $(t_1, m_1, s_1)_q$- and $(t_2, m_2, s_2)_q$-nets, where $k_i = m_i - t_i$ and $s_1 \leq s_2$. Then we can construct a linear $(m_1 + t_2, m_1 + m_2, s_1 + s_2)_q$-net.*

An application of Corollary 1 to nets $(16, 23, 127)_2$ and $(2, 5, 15)_2$ yields a $(21, 28, 142)_2$-net. As a ternary example we obtain an $(11, 22, 23)_3$-net from a $(4, 15, 12)_3$-net and a $(2, 7, 11)_3$-net. A different generalization of the $(u, u + v)$-construction is attempted in [20].

As an example start from $(6, 17, 10)_2$ and apply Corollary 1 with $(3, 8, 10)_2$ as second ingredient. The result is a $(14, 25, 20)_2$-net. More examples will show up in the last section. Just as in coding theory, it is possible to apply Corollary 1 in a recursive fashion.

The $(u, u + v)$-construction can be generalized from the linear case to not necessarily linear ordered orthogonal arrays. The following definition generalizes Definition 5.

Definition 7. *Let $\mathcal{A}$ be an alphabet of size $|\mathcal{A}| = q$. A multisubset $\mathcal{C} \subseteq \mathcal{A}^{(T,s)}$ of size q^m has* **strength** *$k = k(\mathcal{C})$ if k is maximal such that for every ideal K of size k and every k-tuple of entries in K precisely q^{m-k} elements of $\mathcal{C}$ have the prescribed projection to K. We call $\mathcal{C}$ an* **ordered orthogonal array** *OOA of* **length** *s,* **depth** *T,* **dimension** *m and strength k.*

Observe that in the nonlinear case the dimension m need not be integer.

Theorem 5. *Let $\mathcal{A}$ be an alphabet of size $|\mathcal{A}| = q$. For $i = 1, 2$ let $\mathcal{C}_i \subset \mathcal{A}^{(T,s_i)}$ of dimension m_i and strength k_i, where $s_1 \leq s_2$. We can construct $\mathcal{C} \subset \mathcal{A}^{(T,s_1+s_2)}$ of dimension $m_1 + m_2$ and strength $k = \min\{k_2, 2k_1 + 1\}$.*

Proof. We write the elements of $\mathcal{A}^{(T,s)}$ as Ts-tuples with s sections of length T (this is the vector notation mentioned in Section 2). For every pair u, v, where $u \in \mathcal{C}_2$ and $v \in \mathcal{C}_1$, we define a row in $\mathcal{A}^{(T,s_1+s_2)}$ by $r(u,v) = (u, u+v)$. Here we have chosen a structure of an abelian group on $\mathcal{A}$. The addition in $u+v$ is componentwise. The last $s_2 - s_1$ blocks of u have been removed before performing the addition. Let the array $\mathcal{C}$ consist of all these rows $r(u,v)$. We have to show that $\mathcal{C}$ has strength $\geq k$.

Denote the cells of $\mathcal{A}^{(T,s_1+s_2)}$ by (L,i,j), where $i \leq s_2, j \leq T$ (these form the **left part** L) and (R,i,j), where $i \leq s_1, j \leq T$ (the **right part** R). Let K be an ideal of size k. Let $C(K) = \{(i,j) | (R,i,j) \in K \text{ and } (L,i,j) \in K\}$ and $c = |C(K)|$. Let an arbitrary k-tuple be prescribed on the cells from K. The projection of u to the cells from $K \cap L$ are prescribed. Let x be a tuple on $(R, C(K))$ and U_x the set of elements $u \in \mathcal{C}_2$ having the prescribed projection on $K \cap L$ and projecting to x on $(R, C(K))$. Let further V_x be the set of elements $v \in \mathcal{C}_1$ such that $u+v$ has the prescribed projection on $(R, C(K))$. For every $v \in V_x$ let $U_{x,v}$ consist of those $u \in U_x$ such that $u+v$ has the prescribed projection on $(K \cap R) \setminus (R, C(K))$. The pairs (u,v) such that $r(u,v)$ has the required projection on K is then

$$\bigcup_x \bigcup_{v \in V_x} (U_{x,v}, \{v\}).$$

Observe that $c \leq k_1$ as $2c \leq k$. We are done. ∎

It follows that Corollary 1 generalizes from the linear case to arbitrary nets.

6 The finite Gilbert-Varshamov bounds for OOA

Let a code $\mathcal{C} \subseteq \mathbb{F}_q^{(T-1,s)}$ of dimension m and strength k be given. It can be represented as follows: let $a(r), r = 1, \dots m$ be a basis of $\mathcal{C}$. Write the $a(r)$ as rows of a matrix A. The section corresponding to block B_i is $a^{(i)} = (a_1^{(i)}, \dots, a_{T-1}^{(i)})$, where $a_j^{(i)} \in \mathbb{F}_q^m$.

We want to find vectors $a_T^{(i)}$, which complement $\mathcal{C}$ to an m-dimensional code in $\mathbb{F}_q^{(T,s)}$ of strength k. It can be assumed that $a_T^{(i)}, i < s$ have been found already. Our counting condition must be strong enough to guarantee the existence of $a_T^{(s)}$.

Each ideal $K \subset \Omega^{(T,s-1)}$ of size $l \leq k-T$ yields a condition. The number of candidates for $a_T^{(s)}$ excluded by K is q^{T-1} times the number of vectors in $\mathbb{F}_q^{(T,s-1)}$ whose support generates K. We obtain the following:

Theorem 6. *Let $\mathcal{C} \subseteq \mathbb{F}_q^{(T-1,s)}$ of dimension m and strength $\geq k$ be given. Assume*

$$V_{k-T}^{(T,s-1)} < q^{m-T+1},$$

equivalently

$$\sum_{l \leq k-T} \sum_{\pi} (q-1)^b q^{l-b} \binom{s-1}{f_T, \ldots, f_1, s-1-b} < q^{m-T+1},$$

where the sum is over all partitions of l of depth $\leq T$, and b is the breadth of π. Then there is a code $\mathcal{D} \subseteq \mathbb{F}_q^{(T,s)}$ of dimension m and strength $\geq k$, which projects to $\mathcal{C}$.

We mention that Theorem 6 generalizes the strengthened Gilbert-Varshamov bound ([13], p. 34, Theorem 2 of [1]) from Hamming space to NRT-space. It is stronger than the generalization of the ordinary Gilbert-Varshamov bound obtained in [23]. Theorem 6 has the following obvious corollary:

Theorem 7. *Assume $V_{k-T}^{(T,s-1)} < q^{m-T+1}$ holds for $T = 1, 2, \ldots, k-1$. Then there is a linear $(m-k, m, s)_q$-net, equivalently a code $\mathcal{C} \subset \mathbb{F}_q^{(k,s)}$ of dimension m and strength $\geq k$.*

7 Net-embeddable error-correcting codes

Definition 8. *Let $\mathcal{C}$ be a linear code $[s, s-m, k+1]_q$ (equivalently: $\mathcal{C}^\perp \subseteq \mathbb{F}_q^{(1,s)}$ has dimension m and strength $\geq k$). We call $\mathcal{C}$* **net-embeddable** *if there is a linear $(m-k, m, s)_q$-net projecting to $\mathcal{C}^\perp$.*

Recall that we identify linear nets with the corresponding linear subspaces of $\mathbb{F}_q^{(k,s)}$. Net-embeddability is guaranteed if Theorem 6 can be applied recursively, for $T = 2, \ldots, k$. In this section we apply our method in the following form:

Theorem 8. *Assume a linear code $[s, s-m, k+1]_q$ exists and $V_{k-T}^{(T,s-1)} < q^{m-T+1}$ holds for $T = 2, \ldots, k-1$. Then there is an $(m-k, m, s)_q$-net.*

The following lemma simplifies the comparison between the corresponding conditions.

Lemma 1. *Let $V_q(r,n)=V_r^{(1,n)}$ be the volume of a ball of radius r in Hamming space $\mathbb{F}_q^{(1,n)}$. If $n\geq \frac{2q-1}{q-1}r+\frac{q}{q-1}$, then*

$$V_q(r+1,n)\geq qV_q(r,n).$$

Proof. As $V_q(r+1,n)=V_q(r,n)+\binom{n}{r+1}(q-1)^{r+1}$ the claim is equivalent to $V_q(r,n)\leq (q-1)^r\binom{n}{r+1}$. We have $V_q(r,n)=V_q(r-1,n)+\binom{n}{r}(q-1)^r$. By induction we have $V_q(r-1,n)\leq (q-1)^{r-1}\binom{n}{r}$. It suffices to show

$$(q-1)^{r-1}\binom{n}{r}+(q-1)^r\binom{n}{r}\leq (q-1)^r\binom{n}{r+1},$$

equivalently $\binom{n}{r}q\leq\binom{n}{r+1}(q-1)$. We have

$$\binom{n}{r+1}/\binom{n}{r}=(n-r)/(r+1).$$

Our claim is therefore $q(r+1)\leq (q-1)(n-r)$, equivalently $n\geq\frac{2q-1}{q-1}r+\frac{q}{q-1}$. ■

It is easy to see that for strength $k<3$ net-embeddability is always satisfied. In the case of strength 3 we are given a code $[s,s-m,4]_q$. Geometrically this is an $s-$cap in projective space $PG(m-1,q)$. Depth 2 can be reached provided $V_1^{(2,s-1)}=1+(s-1)(q-1)<q^{m-1}$. The depth 3 condition is then automatically satisfied. We conclude that each code $[s,s-m,4]_q$ is net-embeddable provided $s<1+(q^{m-1}-1)/(q-1)$. This has been proved in [24]. The first non-embeddable codes occur in this case when $q=2$ (the extended binary Hamming code is non-embeddable) and in characteristic 2 when $m=3$. The best binary strength 3 net parameters are $(m-3,m,2^{m-1}-1)_2$.

For strength 4 the depth 2 condition is strongest. We conclude that a linear code $[s,s-m,5]_q$ is net-embeddable provided $V_2^{(2,s-1)}<q^{m-1}$. As $V_2^{(2,s-1)}=V_q(2,s-1)+q(q-1)(s-1)$ we arrive at a statement first proved in [25]. The present paper grew out of an attempt to generalize this result.

7.1 Strength 5

Again the depth 2 condition is dominating. This implies that every linear code $[s, s-m, 6]_q$, which satisfies $V_q(3, s-1)+q(q-1)(s-1)V_q(1, s-2) < q^{m-1}$ is net-embeddable.

7.2 Strength 6

It follows from Lemma 1 that the condition for depth 3 is weaker than the depth 2 condition provided $s \geq 12$. The conditions for larger depths are weaker yet. This implies that each linear code $[s, s-m, 7]_q$, $s \geq 12$ which satisfies $V_q(4, s-1) + q(q-1)(s-1)V_q(2, s-2) + q^2(q-1)^2\binom{s-1}{2} < q^{m-1}$ is net-embeddable.

8 Net parameters

We present tables of net parameters $(m-k, m, s)_q$. For $q = 2, 3, 4, 5$ we list k, m, s. Observe that in case $s > m$ the underlying error-correcting code has parameters $[s, s-m, k+1]_q$. As a starting point we used the tables in [5] for $q = 2, 3, 5$. Label t refers to surviving entries from these tables. In some cases when there was a choice we replaced label t by one of the constructions below. Net parameters from [22, 19] are labelled a and b, respectively. The values for strength 3 in the non-binary case follow from cap constructions, see [9]. The label used for nets obtained from embeddings of caps is c. The caps leading to values $(6, 9, 1216)_3$ and $(8, 11, 6464)_3$ are constructed in [7]. Many values for strength $k = 4$ are derived from the families described in [2, 8]. More families of binary nets of moderate strengths based on cyclic codes will be constructed in a forthcoming publication. The corresponding table entries carry the subscript f. The nets with subscript e are computer-constructions obtained by the second author. When $s > m$ starting point is an error-correcting code. Subscript u indicates an application of the $(u, u+v)$-construction. When $s \leq m$ Theorem 7 (pure GV) is applied. The corresponding subscript is g. In case $s > m$ typically we start from a code parameter given in [3] and apply Theorem 8 to prove that it can be embedded in a net. The corresponding entries are marked h.

A class of interesting constacyclic quaternary codes with $d = 5$ were constructed in [10, 6]. We use parameters

$$[85,77,5]_4,\ [171,162,5]_4,\ [341,331,5]_4,\ [683,672,5]_4,\ [1365,1353,5]_4,$$

$$[2731,2718,5]_4,\ [5461,5447,5]_4,\ [10923,10908,5]_4.$$

In some cases, when no better construction seemed available, we used Theorem 7 (subscript g) also when $s > m$. Some good nets can be derived from Theorem 6 starting from $\mathcal{C} \subset \mathbb{F}_q^{(T-1,s)}$ of strength k for $T > 2$. All our examples have $T = 3$. These entries are labelled i. The depth 2 codes $\mathcal{C}$ are derived from linear OA of strength k and length $\geq 2s$ in the most obvious way, by identifying $2s$ coordinates of the space containing the OA with the coordinates of $\Omega^{(2,s)}$. The codes which we used as ingredients can either be obtained from the data base [3] or from primitive BCH-codes. As an example, a $(12,16,3125)_5$-net is based on a $[3125,3109,5]_5$-code, an extended primitive BCH-code.

While we focused attention on linear nets, the tables contain also parameters of nonlinear nets. The only surviving parameters based on nonlinear nets are Mark Lawrence's $(5,21,516)_2$ and $(5,25,2503)_2$ from [12]. They carry subscript L. Finally, we leave a blank for values (k,m) in the tables whenever either we cannot construct a net of length s exceeding the entry in cell $(k,m-1)$ or when we have reached a length of several thousand for a dimension $m' < m$ already.

Notation in tables	
indices	explanation
t	tables from [5]
a	Niederreiter-Xing [22]
b	Niederreiter [19]
c	embedding of caps, see [9]
e	computer embeddings
f	Families from [2, 8]
g	Theorem 7
h	code embedding Theorem 8
i	Theorem 6
u	$(u,u+v)$-construction
L	M. Lawrence's nonlinear nets

q=2

$k\backslash m$	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	7_t	15_t	31_t	63_t	127_t	255_t	511_t	1023_t								
3	3_t	7_t	15_t	31_t	63_t	127_t	255_t	511_t	1023_t	2047_t	4095_t	8191_t				
4		3_t	5_t	8_t	11_t	17_f	23_e	32_e	47_e	65_f	81_h	128_e	151_h	257_f		510_f
5			3_t	5_t	7_t	10_e	14_e	20_e	26_e	36_e	45_e	69_e	77_e	129_f	140_e	257_f
6				3_t	5_t	6_t	9_t	11_t	15_e	21_e	23_e	26_e	36_e	42_e	48_e	64_e
7					3_t	5_t	6_t	7_t	11_t	13_e	16_e	20_e	23_e	28_e	34_e	41_e
8						3_t	5_t	6_t	7_t	9_t	11_e	14_t	16_e	19_e	22_e	26_e
9							3_t	5_t	6_t	7_t	8_t	10_e	12_e	14_e	17_t	20_e
10								3_t	5_t	6_t	7_t	8_t	9_t	11_e	13_e	15_e
11									3_t	5_t	6_t	7_t	8_t	9_t	10_t	12_e
12										3_t	5_t	6_t	7_t	8_t	9_t	10_t
13											3_t	5_t	6_t	7_t	8_t	9_t
14												3_t	5_t	6_t	7_t	8_t
15													3_t	5_t	6_t	7_t

$k\backslash m$	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
4	513_f	1025_f		2046_f	2049_f	4097_f		8190_f	8193_f							
5		513_f	516_L	1025_f		2049_f	2503_L	4097_f		8193_f						
6	72_e	79_e	127_e			130_u	137_h	164_h	196_h	511_f			1023_f			2047_f
7	47_e	58_e	64_e		127_f			133_i	137_i	142_u	511_f			514_u	518_u	526_u
8	30_e	35_e	39_e				42_g	47_g	54_h	64_i	69_h	78_h	89_h	128_i	132_i	133_i
9	23_e	26_e	29_e				34_u	37_u	40_u	46_u	60_i	68_i	71_i	84_i	100_i	113_i
10	17_e	20_t	23_e			24_t	25_t	28_b	31_i	33_i	35_g	40_u	43_g	47_g	52_g	57_g
11	14_e	16_e	18_e				20_u	22_u	24_g	28_b	30_u	33_i	36_u	37_g	40_g	45_i
12	11_e	13_e	15_e				16_g	18_b	19_g	21_g	23_g	28_b		31_g	33_g	36_g
13	10_t	11_e	12_e		13_t	14_t		16_u	18_u	19_u	20_u	22_u	23_g	28_b		30_b
14	9_t	10_t		11_t	12_t	13_t	14_t		15_t		17_t	18_b	20_g	21_g	23_g	28_b
15	8_t	9_t	10_t		11_t	12_t	13_t	14_t		15_t		17_t	18_u	20_u	20_g	22_g

$k\backslash m$	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
6			2050_u	2054_u	2062_u	8191_f										
7	2047_f			2050_u	2054_u	2062_u	8191_f									
8	145_h	163_h	184_h	208_h	234_h	263_h	273_h	274_h	276_h	277_h	294_g	324_g	357_g	394_g	435_g	480_g
9	128_i	134_i		135_i	137_h	152_h	169_h	187_h	208_h	230_h	255_h	282_h	285_h	286_h	287_h	289_g
10	64_i	69_g	76_h	84_h	95_i	128_i	132_i	136_i		146_h	161_h	176_h	193_h	211_h	231_h	253_h
11	50_i	62_i	68_i	71_i	75_i	91_i	100_i	110_i	121_i			122_h	133_h	144_h	156_h	170_h
12	39_g	42_g	45_g	49_g	53_g	58_g	62_g	67_g	73_g	78_g	85_g	91_g	99_g	106_g	115_h	124_h
13	33_g	36_i	38_g	41_g	44_g	47_g	51_g	54_g	64_i	68_i	71_i	72_g	77_g	83_g	89_g	96_g
14		30_b	32_g	35_g	38_i	40_b	43_g	46_g	49_g	52_g	56_g	60_g	64_g	68_g	72_g	77_g
15	23_g	28_b		30_b	32_g	34_b	37_g	40_b	43_i	45_g	48_g	51_g	54_g	57_g	61_g	65_g

q=3

$k\backslash m$	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	13_t	40_t	121_t	364_t	1093_t											
3	4_c	10_c	20_c	56_c	112_c	248_c	532_c	1216_c	2744_c	6464_c						
4		4_t	8_t	14_e	26_f	41_f	80_f	121_f	242_f	365_f	728_f	1093_f	2186_f	3281_f	6560_f	9841_f
5			4_t	7_t	11_e	18_e	28_e	38_e	77_e	95_e	103_e	104_h	151_h	219_h	244_h	245_h
6				4_t	7_t	8_t	13_e	19_e	25_e	33_e	42_e		49_h	65_h	87_h	110_h
7					4_t	7_t	8_t	11_e	15_e	20_e	26_e	34_e		41_i	43_i	53_h
8						4_t	7_t	8_t	10_t	14_e	17_e	22_e			25_g	32_b
9							4_t	7_t	8_t	10_t	12_t	15_e		16_t	18_u	21_g
10								4_t	7_t	8_t	10_t	12_t	13_t	14_t	16_t	
11									4_t	7_t	8_t	10_t	12_t	13_t	14_t	16_t
12										4_t	7_t	8_t	10_t	12_t	13_t	14_t
13											4_t	7_t	8_t	10_t	12_t	13_t
14												4_t	7_t	8_t	10_t	12_t
15													4_t	7_t	8_t	10_t

$k\backslash m$	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
5	660_h	730_h	731_h	1985_h	2188_h	2189_h	5959_h	6562_h	6563_h	6564_h	6565_h	6566_h	6567_h	7262_g	9557_g	
6	120_h	201_h	244_h	245_h	246_h	610_h	729_h	730_h	731_h	1836_h	2187_h	2188_h	2189_h	5514_h	6561_h	6562_h
7	64_h	81_h	121_i	128_h	160_h	200_h	364_i	365_i	390_h	487_h	1093_i	1094_i	1094_i	1179_h	3280_i	3281_i
8	37_h	45_h	54_h	66_h	80_h	96_h	117_h	141_h	170_h	205_h	246_h	247_h	364_i	432_h	520_h	625_h
9	25_g	32_b	35_g	41_g	49_h	58_h	68_h	80_h	95_h	112_h	131_h	155_h	182_h	214_h	245_h	246_h
10	19_t	22_i	25_g	32_b	34_g	40_b	46_g	56_b	61_h	71_h	82_h	95_h	121_i	127_h	146_h	169_h
11		19_t	20_g	23_u	26_g	32_b	34_g	40_b	44_g	56_b	57_g	65_g	74_h	85_h	96_h	110_h
12	16_t		19_t		21_g	24_i	27_i	32_b	34_g	40_b	43_g	56_b		61_g	69_g	78_g
13	14_t	16_t		19_t		20_t	22_t	24_t	28_i	32_b	34_g	40_b	43_g	56_b		59_g
14	13_t	14_t	16_t		19_t		20_t	22_t	24_t	25_g	28_t	32_b	35_g	40_b	42_g	56_b
15	12_t	13_t	14_t	16_t		19_t		20_t	22_t	24_t		28_t	29_g	32_b	35_g	40_b

$k\backslash m$	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
6	6563_h	6564_h	6565_h	6566_h	6862_g	8548_g										
7	3281_i	3284_u	3545_h	4417_h	5503_h	6568_h	6569_h	6570_h	6571_h	6572_h	6573_h	6812_g	8180_g	9824_g		
8	733_h	1093_i	1094_i	1306_h	1569_h	1885_h	3280_i	3281_i			3284_u	3288_u	6567_h	6568_h	6569_h	6570_h
9	247_h	405_h	475_h	556_h	652_h	732_h	733_h			796_g	912_g	1046_g	1200_g	1376_g	1578_g	1809_g
10	194_h	224_h	364_i	365_i	365_i	392_h	451_h	518_h				573_g	647_g	731_g	825_g	932_g
11	125_h	142_h	161_h	183_h	207_h	235_h	248_h	249_h	364_i				400_g	446_g	497_g	555_g
12	88_h	98_h	111_h	118_h	127_h	156_h	175_h	197_h	220_h	247_h	248_h	249_h	273_g	301_g	333_g	367_g
13	66_g	73_g	82_g	91_g	101_h	112_h	125_h	139_h	154_h	171_h	190_h	211_h	234_h	250_h	251_h	263_g
14		57_g	63_g	70_g	77_g	85_g	94_g	104_g	115_h	125_h	139_h	153_h	169_h	186_h	204_h	225_h
15	43_g	56_b			62_g	68_g	74_g	82_g	89_g	98_g	107_g	117_g	128_h	139_h	149_h	168_h

q=4

$k\backslash m$	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	21_t	85_t	341_t	1365_t	5461_t											
3	6_c	17_c	41_c	126_c	288_c	756_c	2110_c	4938_c								
4		5_a	10_e	19_e	32_e	85_e	171_e	373_e	683_e	965_h	1366_h	3861_h	5462_h			
5			5_a	9_a	16_e	26_e	36_e	64_e	81_e	96_h	154_h	245_h	258_h	619_h	983_h	1026_h
6				5_a	9_a	12_e	18_e	26_e	34_e		45_h	65_h	81_h	89_h	187_h	257_h
7					5_a	9_a	10_a	15_e	20_e		22_g	30_u	40_h	53_h	71_h	94_h
8						5_a	9_a	10_a	13_a	17_e		20_a	23_g	29_g	37_h	47_h
9							5_a	9_a	10_a	13_a	15_a	17_a	20_a	21_a	24_g	29_g
10								5_a	9_a	10_a	13_a	15_a	17_a	20_a	21_a	
11									5_a	9_a	10_a	13_a	15_a	17_a	20_a	21_a
12										5_a	9_a	10_a	13_a	15_a	17_a	20_a
13											5_a	9_a	10_a	13_a	15_a	17_a
14												5_a	9_a	10_a	13_a	15_a
15													5_a	9_a	10_a	13_a

$k\backslash m$	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
5	2479_h	3937_h	4098_h	4099_h	4103_u	4119_u	4278_u	6046_g	8549_g							
6	258_h	259_h	753_h	1025_h	1026_h	1027_h	3020_h	4097_h	4098_h	4099_h	4103_u	4114_u	4696_g	6195_g	8174_g	
7	111_h	119_h	219_h	257_h	258_h	259_h	325_g	886_h	1025_h	1026_h	1027_h	1031_u	3554_h	4097_h	4098_h	4099_h
8	60_h	73_h	85_h	95_h	112_h	199_h	252_h	257_h	258_h	292_g	355_g	807_h	1018_h	1025_h	1026_h	1027_h
9	36_g	45_h	55_h	68_h	84_h	94_h	128_i	155_h	190_h	232_h	260_h	261_h	512_i	518_h	632_h	772_h
10	26_a	30_g	36_g	44_g	52_g	63_h	76_h	89_h	101_h	111_h	155_h	186_h	222_h	259_h	260_h	264_g
11		26_a	27_a	31_g	37_g	43_g	51_g	60_g	71_h	83_h	98_h	115_h	125_h	132_g	185_h	217_h
12	21_a		26_a	27_a	28_g	32_g	37_g	43_g	50_g	58_g	68_g	78_h	87_g	98_g	110_g	124_g
13	20_a	21_a		26_a	27_a		29_a	33_a	38_g	44_g	50_g	57_g	66_g	75_g	86_h	98_h
14	17_a	20_a	21_a		26_a	27_a		29_a	33_a	35_g	39_g	44_g	50_g	57_g	65_g	73_g
15	15_a	17_a	20_a	21_a		26_a	27_a		29_a	33_a		36_g	40_g	45_g	51_g	57_g

$k\backslash m$	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
7	4103_u	4114_u	5153_g	6491_g	8178_g											
8	1157_g	3240_h	4084_h	4097_h	4098_h	4099_h	4100_h	4618_g	5629_g	6861_g	8363_g					
9	942_h	1029_h	2048_i	2048_i	2085_h	2543_h	3101_h	3781_h	4102_h	4103_h	4104_h	4105_h	4326_g	5143_g	6116_g	7272_g
10	308_g	535_h	637_h	758_h	903_h	1028_h	1029_h	1030_h	2048_i	2155_h				4101_h	4102_h	4103_h
11	254_h	259_h	260_g	298_g	341_g	391_g	649_h	758_h	885_h	1027_h	1028_h			1176_g	1350_g	1550_g
12	140_g	187_h	215_h	248_h	258_h	259_h	292_g	331_g	374_g	424_g	666_h	766_h			792_g	898_g
13	112_h	128_h	146_h	166_h	189_h	216_h	246_h	261_h	262_h	290_g	325_g	512_i	531_h			574_g
14	83_g	93_g	106_h	119_h	127_g	141_g	171_h	193_h	218_h	245_h	260_h	261_g	290_g	322_g	357_g	397_g
15	64_g	72_g	80_g	90_g	101_g	113_g	124_g	136_g	149_g	164_g	197_h	221_h	246_h	259_h	265_g	291_g

q=5

$k\backslash m$	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	31_t	156_t	781_t	3906_t												
3	6_c	26_c	66_c	186_c	675_c	1715_c	4700_c									
4		6_t	12_e	27_e	44_e	78_e	137_e	138_h	167_g	285_g	625_h	831_g	1421_g	3125_h	4152_g	7099_g
5			6_t	10_t	21_e	33_e	46_e	68_e	96_h	124_h	130_h	156_g	233_g	624_h	625_h	775_g
6				6_t	10_t	14_e	27_e	33_e		44_h	67_h	102_h	130_h	131_h	344_h	515_h
7					6_t	10_t	12_t	25_e			31_u	50_u	57_h	79_h	110_h	131_h
8						6_t	10_t	12_t	16_t	18_t	20_t	22_g	29_g	39_h	52_h	69_h
9							6_t	10_t	12_t	16_t	18_t	20_t	21_t	24_g	30_g	39_g
10								6_t	10_t	12_t	16_t	18_t	20_t	21_t	22_a	26_g
11									6_t	10_t	12_t	16_t	18_t	20_t	21_t	22_a
12										6_t	10_t	12_t	16_t	18_t	20_t	21_t
13											6_t	10_t	12_t	16_t	18_t	20_t
14												6_t	10_t	12_t	16_t	18_t
15													6_t	10_t	12_t	16_t

$k\backslash m$	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
5	1158_g	3124_h	3125_h	3868_g	5784_g	8648_g										
6	627_h	628_h	1727_h	2584_h	3127_h	3128_h	3129_h	3133_u	3877_g	5348_g	7378_g					
7	132_h	163_g	404_h	559_h	627_h	628_h	629_h	2033_h	2805_h	3127_h	3128_h	3129_h	3133_u	4002_g	5233_g	6842_g
8	90_h	119_h	132_h	136_g	171_g	214_g	464_h	608_h	627_h	628_h	668_g	840_g	2335_h	3055_h	3127_h	3128_h
9	50_h	63_h	80_h	102_h	129_h	132_h	148_g	180_g	219_g	267_g	524_h	626_h	627_h	628_h	723_g	883_g
10	32_g	39_g	49_g	60_h	75_h	92_h	113_h	131_h	134_g	159_g	190_g	226_g	269_g	476_h	583_h	626_h
11	23_a	27_g	33_g	40_g	49_g	59_g	71_h	86_h	103_h	125_h	132_h	146_g	171_g	200_g	312_i	373_h
12	22_a	23_a	26_a	29_g	35_g	41_g	49_g	58_g	69_g	82_h	97_h	115_h	132_h	138_g	159_g	183_g
13	21_t	22_a	23_a	26_a	27_a	32_a	37_g	43_g	50_g	58_g	68_g	80_g	93_h	108_h	126_h	133_h
14	20_t	21_t	22_a	23_a	26_a	27_a	32_a	33_g	38_g	44_g	51_g	59_g	68_g	78_g	90_g	104_h
15	18_t	20_t	21_t	22_a	23_a	26_a	27_a	32_a		36_a	40_g	46_g	52_g	60_g	68_g	78_g

$k\backslash m$	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
8	3129_h	3326_g	4186_g	5267_g	6627_g	8340_g										
9	1079_g	2636_h	3126_h	3127_h	3128_h	3129_h	3600_g	4401_g	5381_g	6580_g	8045_g	9837_g				
10	627_h	652_g	779_g	931_g	1112_g	2400_h	2936_h	3126_h	3127_h	3128_h	3244_g	3879_g	4637_g	5545_g	6629_g	7927_g
11	448_h	536_h	629_h	630_h	631_h	712_g	1562_i	1579_h	1889_h	2260_h	2704_h	3130_h	3131_h	3132_h	3133_h	3543_g
12	211_g	243_g	366_h	430_h	507_h	596_h	629_h	630_h	668_g	772_g	893_g	1576_h	1852_h	2177_h	2558_h	3006_h
13	150_g	171_g	195_g	222_g	253_g	288_g	420_h	488_h	565_h	628_h	629_h	638_g	728_g	832_g	951_g	1086_g
14	120_h	132_h	145_g	163_g	183_g	207_g	233_g	263_g	297_g	335_g	476_h	545_h	624_h	628_h	629_h	698_g
15	89_g	101_g	115_h	131_h	141_g	157_g	175_g	196_g	219_g	245_g	274_g	306_g	342_g	469_h	531_h	602_h

References

[1] J. Bierbrauer and Y. Edel: *Lengthening and the Gilbert-Varshamov bound, IEEE Trans. Inform. Theory* **43** (1997), 991-992.

[2] J. Bierbrauer and Y. Edel: *Construction of digital nets from BCH-codes, Monte Carlo and Quasi-Monte Carlo Methods 1996, Lecture Notes in Statistics* **127**(1997), 221-231.

[3] A.E. Brouwer: Data base of bounds for the minimum distance for linear codes, URL http://www.win.tue.nl/∼aeb/voorlincod.html

[4] W.W.L. Chen and M.M. Skriganov: *Explicit constructions in the classical mean squares problem in irregularities of point distributions,* to appear in *J. Reine Angewandte Math.*

[5] A.T. Clayman, K.M. Lawrence, G.L. Mullen, H. Niederreiter and N.J.A. Sloane: *Updated tables of parameters of (t,m,s)-nets, J. Combin. Designs* **7** (1999), 381–393.

[6] I. Dumer and V.A. Zinoviev: *Some new maximal codes over $GF(4)$, Probl. Peredach. Inform* **14** (1978), 24–34, translation in *Problems in Information Transmission* 1979, 174–181.

[7] Y. Edel: *Extensions of generalized product caps,* submitted for publication in *Designs, Codes and Cryptography.*

[8] Y. Edel and J. Bierbrauer: *Families of ternary (t,m,s)-nets related to BCH-codes, Monatsh. Math.* **132** (2001), 99–103.

[9] Y. Edel and J. Bierbrauer: *Large caps in small spaces, Designs, Codes and Cryptography* **23** (2001), 197–212.

[10] D.N. Gevorkyan, A.M. Avetisyan and G.A. Tigranyan: *On the structure of two-error-correcting in Hamming metric over Galois fields,* in: Computational Techniques (in Russian) 3, Kuibyshev 1975, 19–21.

[11] K.M. Lawrence: *A combinatorial characterization of (t,m,s)-nets in base b, J. Combin. Designs* **4** (1996), 275–293.

[12] K.M. Lawrence: *Construction of (t,m,s)-nets and orthogonal arrays from binary codes,* manuscript.

[13] F.J. McWilliams and N.J. Sloane: *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam 1977.

[14] W.J. Martin and D.R. Stinson: *Association schemes for ordered orthogonal arrays and (t,m,s)-nets,* Canadian Journal of Mathematics **51**(1999), 326–346.

[15] G.L. Mullen and W.Ch. Schmid: *An equivalence between* (t, m, s)*-nets and strongly orthogonal hypercubes,* *J. Comb. Theory A* **76** (1996), 164–174.

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

[17] H. Niederreiter: *Point sets and sequences with small discrepancy,* *Monatsh. Math.* **104** (1987), 273–337.

[18] H. Niederreiter: *A statistical analysis of generalized feedback shift register pseudorandom number generators,* *SIAM J. Sci. Statist. Comp.* **8** (1987), 1035–1051.

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

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

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

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

[23] M.Yu. Rosenbloom and M.A. Tsfasman: *Codes for the m-metric,* Problems of Information Transmission **33** (1997),45-52, translated from *Problemy Peredachi Informatsii* **33**(1996),55–63.

[24] W.Ch. Schmid: *(t, m, s)-nets: digital construction and combinatorial aspects,* PhD dissertation, Salzburg (Austria), 1995.

[25] W.Ch. Schmid and R. Wolf, *Bounds for digital nets and sequences, Acta Arith.* **78** (1997), 377–399.

[26] N.J.A. Sloane and D.S. Whitehead: *A new family of single-error correcting codes, IEEE Trans. Inform. Theory* **16** (1970), 717–719.

[27] M.M. Skriganov: *Coding theory and uniform distributions,* to appear in *St. Petersburg Math. J.*, translated from *Algebra i Analiz* **13** (2001), 191–239.