Families of nets of low and medium strength

Jürgen Bierbrauer
Department of Mathematical Sciences, Michigan Technological University, Houghton, Michigan 49931, USA
jbierbra@mtu.edu

Yves Edel
Mathematisches Institut der Universität, Im Neuenheimer Feld 288, 69120 Heidelberg, Germany
y.edel@mathi.uni-heidelberg.de

Received: , Accepted: , Published:

Abstract

The theory of primitive BCH-codes is used to construct linear tms-nets. The codes provide explicit descriptions of ordered orthogonal arrays of low depth. In most cases a Gilbert-Varshamov theorem guarantees the existence of the net. In certain favorable circumstances we obtain explicit descriptions of the nets.

1.Introduction

Equip the Ts-dimensional vector space over $\mathbb{F}_q$ with a basis $\Omega = \Omega^{(T,s)}$ of Ts elements, partitioned into s **blocks** $B_i,\ i = 1, \dots, s$, where each block carries a total ordering

$$\omega_1^i < \omega_2^i < \cdots < \omega_T^i.$$

In this way Ω is the union of s chains (the blocks). An **ideal** of Ω is a subset, which is closed under predecessors.

The vector space with basis Ω becomes a metric space $\mathbb{F}_q^{(T,s)}$ in the following way: write $x = (x_{i,j}) \in \mathbb{F}_q^{(T,s)}$ as a matrix with T rows and s columns. The **weight** $\rho(x)$ is defined as the number of cells remaining after removing the leading zeroes in each column of the matrix x, formally

$$\rho(x) = \sum_{j=1}^{s} T - max\{i | x_{1j} = x_{2j} = \cdots = x_{ij} = 0\}$$

The **distance** is then $d(x, y) = \rho(x - y)$. We studied the metric space $\mathbb{F}_q^{(T,s)}$ in [3] where we called it the Niederreiter-Rosenbloom-Tsfasman space, short NRT-space.

Observe that $\mathbb{F}_q^{(1,s)}$ is the familiar Hamming space of coding theory. An **ordered orthogonal array** (short OOA) of **strength** k is a subspace (a code) $\mathcal{C} \subseteq \mathbb{F}_q^{(T,s)}$ with the property that the projection from $\mathcal{C}$ to any ideal of k cells of $\Omega^{(T,s)}$ is onto.

Here are the basic parameters of an OOA again: it is q-ary if the underlying field is $\mathbb{F}_q$. The **depth** T and **length** s describe the ambient space, the **dimension** $m = dim(\mathcal{C})$ is the dimension as a vector space. The central parameter is the **strength** k.

The strength is a uniformity parameter. A main reason for the interest in OOA is an application in numerical integration, where the q^m elements of the OOA are mapped to points in the s-dimensional unit cube. High strength guarantees that the resulting point set gives a good approximation to the integral. The most important case in this application is $T = k$. An q-ary OOA of strength and depth equal to k is also known as a **tms-net** with parameters $(m-k, m, s)_q$.

Projection shows that the existence of an OOA of depth $T > 1$ implies the existence of an OOA of depth $T-1$, with all other parameters unchanged. Case $T = 1$ corresponds to the well-researched area of error-correcting codes. An OOA of strength k in Hamming space $\mathbb{F}_q^{(1,s)}$ simply is a linear orthogonal array of length s, dimension m and strength k, the dual of a linear $[s, s-m, k+1]_q$-code. It is therefore natural to construct tms-nets by starting from dual codes (depth $T = 1$) and successively embedding OOA of depth T in OOA of depth $T+1$ until depth k is reached. Here the term **embedding** means that an OOA in depth $T+1$ is constructed whose projection to depth T is the given OOA. Call a dual code **net-embeddable** if it can be embedded in a depth k OOA. The resulting net is then an $(m-k, m, s)_q$-net.

The **Gilbert-Varshamov bound** from [3] is a sufficient condition for net embeddability.

Theorem 1 (GV-theorem). *Let $V_l^{(T,s)}$ be the number of elements in $\mathbb{F}_q^{(T,s)}$ of weight at most l. Assume $V_{k-T}^{(T,s-1)} < q^{m-T+1}$.*
Then each depth $T-1$ OOA of strength k can be embedded in depth T (here the established notation is used for the parameters).

Our mainstay will be a construction of OOA in depth 2. The theory of primitive cyclic codes will be used to obtain interesting families of examples. Repeated application of Theorem 1 guarantees the net-embeddability of these depth 2 OOA. Observe that the Department of Mathematics of the University of Salzburg maintains a database of net parameters at http://mint.fh-sbg.ac.at/

2.Cyclic codes, blocks, generator matrices

Each OOA of dimension m is in particular an m-dimensional vector space over $\mathbb{F}_q$ and can therefore be described by a basis. In depth 1 this leads to the well-known description of an m-dimensional code of length s by a generator matrix H_1, an (m,s)-matrix whose rows form a basis of the OOA. Observe that H_1 is a check matrix of the $[s, s-m, k+1]_q$-code obtained by dualization.

An even more natural description is in terms of projective geometry. Each column of H_1 can be interpreted as a point in the $(m-1)$-dimensional projective space $PG(m-1,q)$. In depth T we obtain T such matrices, $H_1,\dots,H_T$, and the geometric description is in terms of Ts projective points, as follows.

Proposition 1. *A q-ary linear m-dimensional OOA of strength k in $\mathbb{F}_q^{(T,s)}$ is equivalently described as follows:*
A family of vectors $X_i(w)\in\mathbb{F}_q^m$, where $i=1,2,\dots,T$ and $w\in W$, $|W|=s$, such that the following holds:
Any subset K of at most k of the vectors $X_i(w)$ is linearly independent provided $X_i(w)\in K, i>1$ implies $X_{i-1}(w)\in K$.

The closure condition $X_i(w)\in K\longrightarrow X_{i-1}(w)\in K$ of Proposition1 reflects the fact that the pairs of indices (i,w) such that $X_i(w)\in K$ should form an ideal. Let $B_w=\{X_1(x),\dots,X_T(w)\}$ be the **block** indexed by $w\in W$. Let $P_i(w)\in PG(m-1,q)$ be the point generated by $X_i(w)$. In geometric terms the defining condition of Proposition1 states that the $P_i(w)$ should be in general position when (i,w) varies in an ideal of at most k elements.

We are going to make use of cyclic codes as ingredients in the construction. Let $F=\mathbb{F}_{q^r}$ be an extension field, s a divisor of q^r-1 and W the subgroup of order s of the multiplicative subgroup of F. In most cases we will choose $s=q^r-1$. This is known as the **primitive** case. Let $A\subset\mathbb{Z}/s\mathbb{Z}$ be a set of **exponents.** The set $\mathbb{Z}/s\mathbb{Z}$ of exponents is partitioned into **cyclotomic cosets.** Denote by $Z(i)$ the cyclotomic coset containing i. The **Galois closure** $\tilde{A}$ of A is the union of all $Z(i),\ i\in A$. The smallest subfield $L\subseteq F$ containing all $w^i,\ w\in W$ is the extension of degree $|Z(i)|$ of $\mathbb{F}_q$. We interpret w^i not as elements of F but as q-ary $|Z(i)|$-tuples. A matrix M with s columns is constructed as follows: for each cyclotomic coset intersecting A nontrivially choose a representative i. The entry of M in row i and column w is w^i, where w^i is interpreted as a q-ary $|Z(i)|$-tuple as above. It follows that M is a matrix with $\sum_i|Z(i)|$ rows and s columns, with entries in $\mathbb{F}_q$.

Let $I=\{a,a+j,a+2j,\dots\}\subset\mathbb{Z}/s\mathbb{Z}$ be a set of exponents, which form an arithmetic progression (calculation is mod s). Then I is an **interval** if the stepwidth j is coprime to s. The **BCH-bound** of coding theory states the following: if $\tilde{A}$ contains an interval I, then any set of $|I|$ columns of matrix M is linearly independent. In other words, M is the check matrix of a code with minimum distance $> |I|$.

Definition 1. *Let $X_w \in \mathbb{F}_q^m$ where $w \in W, |W| = s$. The family X_w is* **k-wise independent** *if any k of the X_w are linearly independent.*

With this terminology the BCH-bound states that the family of columns of matrix M above is $|I|$-independent if the Galois closure of the set of exponents contains an interval I.

3.A construction in depth 2

Theorem 2. *Let W be an index set of s elements. For every $w \in W$ let $X_1(w) = (A_w, B_w, 0) \in \mathbb{F}_q^m$ and $X_2(w) = (0, B_w, C_w) \in \mathbb{F}_q^m$ such that the following are satisfied:*

1. *The $X_1(w)$ are k-wise independent,*
2. *the C_w are l-wise independent,*
3. *the B_w are $(k-l-1)$-wise independent,*
4. *the (A_w, C_w) are $\lfloor (k/2) \rfloor$-wise independent.*

Then the $X_1(w), X_2(w)$ generate an OOA of strength k in $\mathbb{F}_q^{(2,s)}$

Proof. Consider a linear dependency involving both vectors of some i blocks and only the first vector of some $k-2i$ blocks, where $i = 0, 1, \ldots, \lfloor (k/2) \rfloor$. The first assumption yields a contradiction when $i = 0$. The l-wise independence leads to a contradiction when $0 < i \leq l$. Let $i \geq l+1$. The number of blocks involved is $\leq k-l-1$. The independence property of the B_w shows that $\alpha_j = -\beta_j$ for $j = 1, \ldots, i$ and $\alpha_j = 0$ for $j > i$. Observe $i \leq \lfloor (k/2) \rfloor$. The assumption on the (A_w, C_w) yields a contradiction. □

We use cyclic codes to obtain the ingredients of Theorem 2. In particular we concentrate on the primitive binary case, where $F = \mathbb{F}_{2^r}$ and W is the multiplicative group of F. We fix notation in order to have a succinct expression in cases when Theorem 2 is applied to primitive cyclic codes.

Definition 2. *Let $\mathbb{F}_q$ be the ground field, $F = \mathbb{F}_{q^r}$ and $W = F \setminus \{0\}$. Let $I = (a|b|c)$, where a, b, c are strings of integers mod $q^r - 1$. Define $X_1(w) = (A_w, B_w, 0) \in \mathbb{F}_q^m$ and $X_2(w) = (0, B_w, C_w) \in \mathbb{F}_q^m$, where $A_w = w^a, B_w = w^b, C_w = w^c$ and w^a stands short for the tuple $(w^{a_1}, \ldots, w^{a_i})$ if $a = (a_1, \ldots, a_i)$, analogously for the other exponents.*

Define $X(I)$ of depth 2, length $s = q^r - 1$, whose block w is defined by $X_1(w), X_2(w)$. Call I the **vector of exponents.** *The dimension m is determined as $m = m_a + m_b + m_c$, where $m_a = \sum_{j=1}^{i} |Z(a_j)|$, analogousy for m_b, m_c.*

Theorem 2 shows that we can read off the strength of $X(I)$ from the set of exponents I.

Proposition 2. *Let u be a string of integers mod $s = q^r - 1$. We say that u* **generates strength** *k if the vectors $w^u, w \in W = F \setminus \{0\}$ have this property (see Definition 1). Here we use the same convention as in Definition 2. Let $X(I)$ be as in Definition 2, where $I = (a|b|c)$ is the vector of exponents. It follows from Theorem 2 that $X(I)$ has strength k provided the following hold:*

1. *$(a|b)$ generates strength k,*
2. *c generates strength l,*
3. *b generates strength $(k - l - 1)$, and*
4. *$(a|c)$ generates strength $\lfloor (k/2) \rfloor$.*

If the conditions of Proposition 2 are satisfied we call I a **vector of exponents of strength k in depth** 2.

The BCH bound implies that a vector u of integers generates strength k provided the Galois closure of u contains an interval of k integers. Observe also that in the binary case a string $u = (i)$ consisting of just one integer i generates strength 2 provided i is coprime to $2^r - 1$. This follows from the fact that the Galois closure contains $\{i, 2i\}$, an interval of length 2.

As a first illustration of Proposition 2 consider the vector $I = (-1|0, 1|0)$ in the binary case $q = 2$. The conditions of Proposition 2 are satisfied for $k = 5, l = 1$. For example, $(a|b)$ generates strength 5 as the Galois closure of $\{-1, 0, 1\}$ (obtained by repeated multiplication by 2) contains the interval $\{-2, -1, 0, 1, 2\}$, and $(a|c)$ generates strength $\lfloor 5/2 \rfloor = 2$ as the closure of $\{-1, 0\}$ contains the interval $\{-2, -1, 0\}$: in fact strength 3 is generated. The dimension is the sum of the lengths of the cyclotomic cosets involved, where each section is counted seperately: $m = |Z(-1)| + |Z(0)| + |Z(1)| + |Z(0)| = r + 1 + r + 1 = 2r + 2$. This yields an OOA of depth 2, strength $k = 5$ and dimension $m = 2r + 2$, where $s = 2^r - 1$. The Gilbert-Varshamov bound Theorem 1 shows that $X(I)$ is net-embeddable. This yields a $(2r - 3, 2r + 2, 2^r - 1)_2$-net for all r, duplicating a result from [4]. Slightly better parameters are obtained in [2], where BCH-codes of length $2^r + 1$ are used to construct $(2r - 3, 2r + 2, 2^r + 1)_2$-nets.

The following is a direct application of Proposition 2:

Theorem 3. *Let $q = 2$. The following are vectors of exponents of strength k in depth* 2.

- $I = (-(2v - 1), \ldots, -1, 0|1, 3, \ldots, 6v - 1|1, 3, \ldots 2v - 1)$
  for $k = 8v + 1, v \geq 1$.

- $I = (-(2v-1), \ldots, -1, 0|1, 3, \ldots, 6v+1|1, 3, \ldots 2v-1)$ *for* $k = 8v+3, v \geq 1$.

- $I = (-(2v+1), \ldots, -1|0, 1, 3, \ldots, 6v+1|0, 1, 3, \ldots 2v-1)$ *for* $k = 8v+5, v \geq 1$.

- $I = (-(2v+1), \ldots, -1|0, 1, 3, \ldots, 6v+3|0, 1, 3, \ldots 2v-1)$ *for* $k = 8v+7, v \geq 1$.

Proposition 2 may be seen as an attempt to embed the OA (depth 1) defined by exponents $(a|b)$ in an OOA of depth 2, while inflating the dimension. This is not interesting at all if the original OA is embeddable. In general we wish to keep the contribution of the additional exponents c as low as possible. For large strengths Proposition 2 cannot be expected to give good results as in these cases the strength is roughly proportional to the number of exponents and it is easy to see that the best choice for l under this assumption is about one quarter of the strength, as in Theorem 3. For large strength this leads to uninteresting dimensions. For small and medium strengths however Proposition 2 leads to a large number of good nets, in particular in the binary case. The last step involves embedding the OOA at depth 2 in a net, either by applying the GV-bound Theorem 1 or by describing an explicit embedding. In order to apply the GV-bound we need a better understanding of the parameters involved in Theorem 1.

Lemma 1. *The volume of the unit ball of radius l in the metric on $\mathbb{F}_q^{(T,s)}$ is $V_l^{(T,s)} = \sum_{i=0}^{l} S_i^{(T,s)}$, where*

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

the sum is over all partitions π of l with largest part $\leq T$, f_i is the multiplicity of i as a part of π and $b = \sum f_j$.

4.Binary nets of strength 6

The first application of Proposition 2, which is of independent interest, occurs for strength 6.

Theorem 4. *If $q = 2$ and r is not divisible by 4, then $I_1 = (5|1, 3|0)$ is a vector of exponents of strength 6 in depth 2. The corresponding OOA $X(I_1)$ has dimension $m = 3r+1$ in $\mathbb{F}_q^{(2,s)}$, where $s = 2^r - 1$.*

The vector $I_2 = (-1, 0|1, 3|0)$ of dimension $m = 3r+2$ has strength 6 in depth 2 for all r.

These depth 2 OOA are embeddable into nets. The resulting binary linear nets have parameters $(3r-5, 3r+1, 2^r-1)_2$ *when* r *is not a multiple of* 4, *parameters* $(3r-4, 3r+2, 2^r-1)_2$ *for arbitrary* r.

Proof. The conditions of Proposition 2 are satisfied for $k=6, l=1$. In the case of I_1 we have that $(a|c)=(5,0)$ generates strength 3 as $\{0,5,10\}$ is an interval. This is where the assumption on r is needed. We have reached depth 2. The GV-theorem shows net-embeddability In fact, the condition is tightest for embedding into depth 3. It reads $V_{k-T}^{(T,s-1)} < q^{m-T+1}$, where $q=2, T=3, s=2^r-1$. The critical case is $m=3r+1$. The right side is 2^{3r-1}, the dominating term on the left occurs when $b=3$, hence $l=3, f_1=3$. This dominating term is therefore $\binom{s-1}{3,s-4}=\binom{s-1}{3}\sim 2^{3r}/6$. □

Theorem 4 yields in particular nets $(22,28,511)_2$, $(25,31,1023)_2$ and $(28,34,2047)_2$. These parameters are reported in [3] already. An alternative direct construction allows us to improve on Theorem 4.

Theorem 5. *Let* $F=\mathbb{F}_{2^r}$. *The vectors*

$$X_1(w)=(0,w,w^3,w^5),\ \ X_2(w)=(1,w,w^3,w^5+w)$$

generate an OAA of strength 6, *depth* 2 *and dimension* $3r+1$.

Proof. The BCH-bound and the first coordinate show that we can assume that no more than 4 blocks are involved in a linear dependency. The first coordinate shows that the only critical case is when precisely 4 blocks are involved. As exponents 1, 3 generate strength 4 it suffices to consider a linear dependency of $X_1(x), X_2(x), X_1(y), X_2(y)$ for some $x\neq y$. Let the coefficients be a,b,c,d. Because of strength 4 we have $a+b=c+d=0$. The first coordinate shows $b+d=0$. The coefficients are $a,-a,-a,a$. The last coordinate section shows $0=-ax+ay=a(y-x)$, hence $a=0$. □

Corollary 1. *A* $(3r-5, 3r+1, 2^r-1)_2$*-net exists for all* r.

This yields in particular a $(19,25,255)_2$-net.

5.Binary nets of strength 7

Theorem 6. *Let* $q=2$. *If* r *is not divisible by* 4, *then* $I_1=(5|0,1,3|0)$ *is a vector of exponents of strength* 7 *in depth* 2. *In particular* $X(I_1)$ *generates of code of strength* 7 *and dimension* $m=3r+2$ *in* $\mathbb{F}_q^{(2,s)}$, *where* $s=2^r-1$.

The vector $I_2=(-1,0|0,1,3|0)$ *has strength* 7 *in depth* 2 *for arbitrary* r. *The dimension is* $m=3r+3$.

Proof. Apply Proposition 2 in case $k = 6, l = 1$. $\square$

When r is odd we can construct an explicit embedding in depth 3. The proof makes use of a special case of the following lemma, which is proved in [5].

Lemma 2. *Let $gcd(r, h) = 1$. Then $\{0, 1, 2^h + 1\}$ generates strength 4. In particular exponents $\{0, 1, 5\}$ generate strength 4 when r is odd.*

Theorem 7. *For every odd r there is a linear $(3r - 5, 3r + 2, 2^r - 1)_2$-net.*

Proof. If $q = 2$ and r is odd, we construct an explicit embedding of the family in Theorem 6 defined by I_1 in an OOA of depth 3. The GV embedding theorem proves the claim.

Recall

$$X_1(w) = (w^5, 1, w, w^3, 0),\ X_2(w) = (0, 1, w, w^3, 1).$$

We choose $X_3(w) = (0, 1, w, 0, 1)$.

Here and in the sequel we consider non-trivial vanishing linear combinations of the $X_j(w_i)$. Denote the coefficient of $X_1(w_i)$ by α_i, of $X_2(w_i)$ by β_i and so forth. The **type** of the linear combination is a partition of k. For example, in the case of type $(3, 1, 1, 1, 1)$ the coefficients are $\gamma_1, \beta_1, \alpha_1, \ldots, \alpha_5$. Clearly $\gamma_1 = 1$. The last coordinate shows $\gamma_1 = \beta_1 = 1$. The second coordinate section shows that there is an even number of non-vanishing coefficients α_i. Assume $\alpha_1 = 0$. The contribution of the first block is $(0, 0, 0, w_1^3, 0)$. Exponents $\{0, 1, 5\}$ yield strength 4 (see Lemma 2). Here we use the hypothesis that r is odd. The first three coordinate segments show $\alpha_i = 0$ for $i > 1$, contradiction. We have $\gamma_1 = \beta_1 = \alpha_1 = 1$ and we can assume $\alpha_5 = 0$. The contribution of the first block is $(w_1^5, 1, w_1, 0, 0)$. The same argument as before yields a contradiction.

Consider type $(3, 2, 1, 1)$. Clearly $\gamma_1 = \beta_2 = 1$. The last coordinate shows $\beta_1 = 0$ and because of the second coordinate there is an even number of non-vanishing α. Assume $\alpha_1 = 1$. The fact that exponents $0, 1$ generate strength 3 shows $\alpha_3 = \alpha_4 = 0, \alpha_2 = 1$. Exponent 3 yields a contradiction. We have $\alpha_1 = 0$. If $\alpha_2 = 1$, the strength 3 argument yields a contradiction. We have $\alpha_2 = 0$. The contribution of the first two blocks is $X_3(w_1) + X_2(w_2)$. Exponent 5 shows $\alpha_3 = \alpha_4 = 0$, exponent 1 yields a contradiction.

In type $(3, 2, 2)$ we have $\beta_2 = \beta_3 = 1$, because of the strength 3 argument $\alpha_2 = \alpha_3 = 1$ and then $\gamma_1 = 1, \beta_1 = 1, \alpha_1 = 0$. The contradiction $w_1^3 = 0$ is obtained.

The final type is $(3, 3, 1)$. The strength 3 argument shows $\alpha_3 = 0$. Clearly $\gamma_1 = \gamma_2 = 1$. Exponent 5 shows $\alpha_1 = \alpha_2 = 0$. The strength 3 argument shows $\beta_1 = \beta_2 = 1$. Exponent 3 yields a contradiction. Here the hypothesis that r is odd is needed again. $\square$

As examples of Theorem 7 we obtain nets

$$(16, 23, 127)_2,\ (22, 29, 511)_2,\ (28, 35, 2047)_2,$$

which were announced in [3] already. Instead of invoking Theorem 1 it is preferable to obtain an explicit construction of the net embedding. Whenever r is not a multiple of 3 this can be done for the depth 3 OAA constructed in the proof of Theorem 7. In the proof of Theorem 8 we make use of another independence result for sets of exponents which is not implied by the BCH-bound.

Lemma 3. *If r is not a multiple of 3, then the set $\{3,5\}$ of exponents has strength ≥ 3.*

Proof. As $5,6$ is contained in the defining set, strength 2 is guaranteed by the BCH-bound. By the assumption on r the set $\{0,7\}$ is an interval. As $\{3,5\}+\{0,7\}$ is in the defining set it follows from the Roos bound [6] from the theory of cyclic codes that the strength is ≥ 3. The computer shows that in case $r=9$ the strength is indeed $=2$, thus indicating that the assumption on r is necessary. $\square$

Theorem 8. *Let $q=2$ and r coprime to 6. A net embedding of the depth 3 codes from the proof of Theorem 7 is described by*

$$X_4(w)=(0,1,w,0,0),\ X_5(w)=(0,1,0,0,0),\ X_6(w)=(0,1,aw,0,0),$$

where $a\notin\mathbb{F}_2$.

Proof. Recall

$$X_1(w)=(w^5,1,w,w^3,0),\ X_2(w)=(0,1,w,w^3,1),\ X_3(w)=(0,1,w,0,1).$$

Consider type $(4,1,1,1)$. Clearly $\delta_1=1$. The last coordinate shows $\beta_1=\gamma_1$. If both are $=1$ the fact that exponents $1,3$ generate strength 4 shows $\alpha_2=\alpha_3=\alpha_4=0$, contradiction. We have $\beta_1=\gamma_1=0$. Assume $\alpha_1=1$. The contribution of the first block is $(w_1^5,0,0,w_1^3,0)$. As exponents $0,1$ generate strength 3 it follows $\alpha_2=\alpha_3=\alpha_4=0$, contradiction. We have $\alpha_1=0$ and $X_4(w_1)$ is the contribution of the first block.

As r is not a multiple of 3 exponents $3,5$ generate strength 3 (see Lemma 3). This implies $\alpha_2=\alpha_3=\alpha_4=0$, contradiction.

Consider type $(4,2,1)$. Exponents $0,1$ show that $\alpha_3=0,\alpha_2=\beta_2$ and that $(\alpha_1,\beta_1,\gamma_1)$ has odd weight. Exponent 3 shows $\alpha_1=\beta_1$, hence $\gamma_1=1$. Exponent 5 shows $\alpha_2=\beta_2=0$ and $\alpha_1=0$. We have reached a contradiction.

The final type in depth 4 is $(4,3)$. Clearly $\gamma_2=1$. Exponents $0,1$ show $\alpha_2\neq\beta_2$ and $(\alpha_1,\beta_1,\gamma_1)$ has odd weight. Exponent 3 yields $\alpha_1=\beta_1$, hence $\gamma_1=1$, as well as $\alpha_2=\beta_2$, contradiction.

We have reached depth 4. Consider type $(5,1,1)$. The last coordinate shows $\beta_1=\gamma_1$. The first segment shows $\alpha_2=\alpha_3$. The second segment shows that $(\alpha_1,\beta_1,\gamma_1,\delta_1)$ has odd weight. Assume at first $\alpha_2=\alpha_3=0$. Exponents 3 and 5 show $\alpha_1=0=\beta_1=\gamma_1,\delta_1=1$, contradiction. We have $\alpha_2=\alpha_3=1$. Exponent 5 shows $\alpha_1=1$. We have that $(\beta_1,\gamma_1,\delta_1)$

has even weight, the second segment implies $\beta_1 = 0, \gamma_1 = \delta_1$, the second segment shows $\beta_1 = \gamma_1 = \delta_1 = 0$. The fact that exponents $1, 3$ generate strength 3 yields a contradiction.

Consider type $(5, 2)$. Clearly $\epsilon_1 = \beta_2 = 1$. The last segment shows $\beta_1 \neq \gamma_1$, the third segment shows $\alpha_2 = 1$ and $(\alpha_1, \beta_1, \gamma_1, \delta_1)$ has even weight. The fourth segment implies $\alpha_1 = \beta_1$, hence $\gamma_1 = \delta_1$. Exponent 5 yields a contradiction. We have reached depth 5.

The only type to consider in depth 6 is $(6, 1)$. The third segment shows $\alpha_2 = 1$. Exponent 5 shows $\alpha_1 = 1$ and $w_1^5 = w_2^5$, a contradiction as r is odd. $\square$

Theorem 9. *Let $q = 2$. Then $I_3 = (-1|0, 1, 3|0)$ is a vector of exponents of strength 7 in depth 2. An embedding in depth 3 is defined by*
$X_3(w) = (w^{-1}, 0, 0, w, 1)$.

Proof. In depth 2 this is another application of Proposition 2 for $k = 6, l = 1$. Consider type $(3, 1, 1, 1, 1)$. The last coordinate shows that $X_3(x)$ and $X_2(x)$ are involved in the linear combination where x is the block at depth 3. As $X_3(x) + X_2(x) = (x^{-1}, 1, x, x, 0)$ and exponents $-1, 0, 1$ generate strength 5 it follows that the linear relation involves only block x. The penultimate coordinate section yields a contradiction. Consider type $(3, 2, 1, 1)$. The last coordinate and the fact that type $(3, 1, 1, 1, 1)$ has been dealt with shows that with obvious terminology $X_3(x)$ and $X_2(y)$ must be involved in the linear relation while $X_2(x)$ is not. Exponents $0, 1$ generate strength 3. If $X_1(x)$ is not involved it follows that only blocks x, y are used. The first section yields a contradiction. If $X_1(x)$ is involved the contribution of the x-block is $(0, 1, x, x, 1)$. If $B_1(y)$ is involved the strength 3 argument yields a contradiction again. The contribution of block y is therefore $X_2(y) = (0, 1, y, y^3, 1)$. The first coordinate section shows that the remaining vectors at depth 1 cannot be involved. As $x \neq y$ this is a contradiction. The remaining types are easily excluded. In type $(3, 2, 2)$ the sum of all 7 vectors must vanish which is impossible because of the first section. In type $(3, 3, 1)$ the vector in the block at depth 1 is not involved and the sum of the remaining 6 vectors must vanish which is not the case because of the penultimate coordinate section. $\square$

The OOA of Theorem 9 can be embedded into nets. This yields the following improvement upon Theorem 7:

Corollary 2. *For every r there is a linear $(3r - 5, 3r + 2, 2^r - 1)_2$-net.*

This yields net parameters

$$(13, 20, 63)_2,\ (19, 26, 255)_2,\ (25, 32, 1023)_2,\ (31, 38, 4095)_2.$$

6.Binary nets of strengths 8

Theorem 10. *Let $F = \mathbb{F}_{2^r}$. The vectors*

$$X_1(w) = (0, w, w^3, w^5, w^7),\ X_2(w) = (w, w, w^3, w^5, w^7 + w^3)$$

generate an OAA of strength 8*, depth* 2 *and dimension* $5r$*.*

Proof. Depth 1 is obvious because of the BCH-bound, types $(2, 1, 1, 1, 1, 1, 1)$ and $(2, 2, 1, 1, 1, 1)$ are OK because of the first coordinate section. In the remaining types the exponents $1, 3, 5$ show that for each block at depth 2 both vectors must be involved. As $X_1(x) + X_2(x) = (x, 0, 0, 0, x^3)$ and exponents $1, 3$ generate strength 4 we see that those types are excluded. □

The OOA of Theorem 10 are net-embeddable by Theorem 1.

Corollary 3. $(5r - 8, 5r, 2^r - 1)_2$*-nets exist for all* r*.*

7. Binary nets of strengths 9 and 11

Theorem 3 shows that $I = (-1, 0|1, 3, 5|1)$ is a vector of exponents of strength 9 and $I = (-1, 0|1, 3, 5, 7|1)$ is a vector of exponents of strength 11. The dimensions are $m = 5r + 1$ and $m = 6r + 1$, respectively.

The GV theorem does not suffice to guarantee a net embedding in general. In the case of the strength 9 family nets $(5r - 8, 5r + 1, 2^r - 1)_2$ are obtained for $r \leq 8$.

Proposition 3. *For every* r *there is a binary OOA of dimension* $5r + 2$ *and strength* 9 *at depth* 3*.*

Proof. We use the family of depth 2 and strength $k = 9$ as constructed above with an additional final bit coordinate, explicitly

$$X_1(w) = (w^{-1}, 1, w, w^3, w^5, 0, 0),\ X_2(w) = (0, 0, w, w^3, w^5, w, 0),$$

and we choose

$$X_3(w) = (0, 1, w, w^3, w^5, 0, 1).$$

The last bit yields a contradiction whenever entry 3 occurs an odd number of times in the type. The first type to consider is therefore $(3, 3, 1^3)$. Because of exponents $1, 3, 5$ only the blocks at depth 3 are involved in the linear relation. The first coordinate section shows that the vectors at depth 1 are not involved, the penultimate section shows that the depth 2 vectors are not involved, contradiction.

The situation is similar in type $(3,3,2,1)$. The depth 1 block does not contribute. The first section shows that each depth 3 block contributes the vectors at depth 1 and 3 to the linear relation. This is impossible because of the second section. □

Corollary 4. *A $(5r-7, 5r+2, 2^r-1)_2$-net exists for all r.*

Proof. Apply the GV embedding theorem to Proposition 3. □

In the same manner, the strength 11 family yields nets

$$(32, 43, 121)_2 \text{ and } (38, 49, 210)_2.$$

Proposition 4. *Whenever r is not a multiple of 3 there is a binary OOA of dimension $6r+2$, strength 11 and depth 3.*

Proof. Use the family of depth 2 and strength $k = 11$ as constructed earlier with an additional final bit coordinate, explicitly

$$X_1(w) = (w^{-1}, 1|w, w^3, w^5, w^7|0|0),\ X_2(w) = (0, 0|w, w^3, w^5, w^7|w|0),$$

and we choose

$$X_3(w) = (0, 0|w, w^3, w^5, 0|w|1).$$

The last bit shows that we need to consider only types containing an even number of entries 3. The first type to consider is $(3,3,1^5)$. We have $\gamma_1 = \gamma_2 = 1$. The penultimate section (exponent 1) shows $\beta_1 = \beta_2 = 1$. Assume $\alpha_1 = 0$ or $\alpha_2 = 0$. As exponents $1,3,5$ generate strength 6 we obtain $\alpha_i = 0$ for all i. Exponent 7 yields a contradiction as 7 does not divide the group order. We have $\alpha_1 = \alpha_2 = 1$. Exponents $-1,0,1,3,5$ yield a contradiction.

All remaining types have ≤ 6 parts. As exponents $1,3,5$ generate strength 6 we can assume that parts 1 do not occur in the type. In type $(3,3,2)$ we have $\alpha_3 = \beta_3 = 1$. Exponents $-1,0$ yield a contradiction.

The last type to exclude is $(3,3,2,2)$. Exponents $1,3,5$ show $\alpha_3 = \beta_3 = \alpha_4 = \beta_4 = 1$. If $\alpha_1 = 0$ or $\alpha_2 = 0$, exponents $-1,0$ would yield a contradiction. Because of exponents $1,3,5$ we conclude $\alpha_1 = \alpha_2 = 1, \beta_1 = \beta_2 = 0$. Exponent 7 yields a contradiction as r is not a multiple of 3. □

Proposition 4 is not sufficient to guarantee a net embedding in general.

References

[1] J.Bierbrauer: *The theory of cyclic codes and a generalization to additive codes, Designs, Codes and Cryptography* **25** (2001), 189-206.

[2] J.Bierbrauer: *A family of binary* (t, m, s)*-nets of strength* 5, *Designs, Codes and Cryptography*, to appear.

[3] J.Bierbrauer, Y.Edel and W.Ch.Schmid: *Coding-Theoretic constructions for tms-nets and ordered orthogonal arrays, Journal of Combinatorial Designs* **10** (2002), 403-418.

[4] T.Helleseth, T. Klove and V. Levenshtein: *Hypercubic* 4*-and* 5*-designs from double-error-correcting BCH codes, Designs, Codes and Cryptography* **28** (2003), 265-282.

[5] Henk D.L.Hollmann and Q.Xiang: *Maximal arcs in projective three-spaces and double-error-correcting cyclic codes, Journal of Combinatorial Theory A* **93**(2001),168-172.

[6] C.Roos: *A new lower bound for the minimum distance of a cyclic code, IEEE Transactions on Information Theory* **29** (1983),330-332.

[7] W.Ch.Schmid: *Shift-nets: a new class of binary digital* (t, m, s)*-nets,* in *Monte Carlo and Quasi-Monte Carlo Methods 1996, Lecture Notes in Statistics* **127** (1997), 369-381.