Hypercubic 4 and 5-Designs from Double-Error-Correcting BCH Codes *

Tor Helleseth and Torleiv Kløve,
Department of Informatics, University of Bergen
HIB, N-5020 Bergen, Norway,

Vladimir I. Levenshtein,
Keldysh Institute for Applied Mathematics, RAS,
Miusskaya sq. 4, 125047 Moscow, Russia.

Abstract

An ordered orthogonal array OOA(τ, k, n) is a binary $2^k \times n\tau$ matrix with the property that for each complete τ-set of columns, each possible τ-tuple occurs in exactly $2^{k-\tau}$ rows of those columns (for definition of a complete τ-set, see below). Constructions of OOA(τ, k, n) for $\tau = 4$ and $\tau = 5$ are given.

1 Introduction. Hypercubic Designs and Ordered Orthogonal Arrays

In this introduction we give an overview of the related concepts hypercubic τ-design, (t, k, n)-nets, and ordered orthogonal array. We also give necessary definitions and formulate our results.

Consider the unit continuous hypercube $I^n = [0, 1)^n$. We call a parallelogram $P \subseteq I^n$ *binary rational* if it is a product of n half-open intervals $[\frac{a}{2^m}, \frac{a+1}{2^m})$ for some $m = 0, 1, \ldots$ and $a = 0, 1, \ldots, 2^m - 1$. The volume of a

*The research was supported by the Norwegian Research Council and the Russian Foundation for Basic Research under grant 01-01-00035.

parallelogram is the product of the lengths of the intervals and for any τ, $\tau = 0, 1, \ldots$, there are exactly $2^\tau \binom{n+\tau-1}{\tau}$ binary rational parallelograms of volume $2^{-\tau}$. We call a subset C of 2^k points of $[0,1)^n$ an (n,k) *hypercubic τ-design* if any binary rational parallelogram of volume $2^{-\tau}$ contains exactly $2^{k-\tau}$ points of C. This notion in an equivalent form was introduced and studied by Sobol' [14] in 1967 in connection with the investigation of the following approximation formula

$$\int_0^1 \cdots \int_0^1 f(x)dx_1 \cdots dx_n \approx \frac{1}{2^k} \sum_{x \in C} f(x).$$

Niederreiter [11] extended the notion of (binary) hypercubic τ-designs to the alphabet of b symbols and called them $(k-\tau, k, n)$-nets in base b, a terminology which has been broadly used in the further literature.

It is clear that if in the binary rational representation of all 2^k points of a hypercubic τ-design $C \subset [0,1)^n$ we remove all digits after the comma except for the first τ, then this set of 2^k points preserves the property of being a τ-design (removing the digits just has the effect of moving the points such that the corresponding projections on the intervals are moved from somewhere in the intervals to the left endpoint of the intervals). Therefore, a natural problem is to give a combinatorial interpretation of binary matrices of size $2^k \times (\tau n)$ which give a hypercubic τ-design. This problem was set by Niederreiter in [11] and he was close to its solution. However, a complete solution of this problem was found later independently by Lawrence [4] and Mullen and Schmid [10]. Rozenblyum and Tsfasman [13] introduced an ordered Hamming weight (norm) and, for the corresponding metric space, considered the traditional coding theory problems to construct codes with a given minimum distance and estimate their maximum size. This ordered norm turned out to be a natural base for describing the combinatorial interpretation of hypercubic designs and is defined as follows.

We denote by $GF(2)^\tau$ the set of binary vectors $\mathbf{u} = (u_1, u_2, \ldots, u_\tau)$; we also write $\mathbf{u} = u_1 u_2 \ldots u_\tau$ considering $\mathbf{u}$ as a word of length τ over the alphabet $GF(2) = \{0, 1\}$. For $\mathbf{u} = u_1 u_2 \ldots u_\tau \in GF(2)^\tau$, let $w(\mathbf{u}) = \max\{i \mid u_i = 1\}$ for $\mathbf{u} \neq \mathbf{0}$, and $w(\mathbf{0}) = 0$. The *ordered τ-weight* w_τ is defined on the set $GF(2)^{\tau n}$ of binary vectors (words) of length τn and equals $w_\tau(\mathbf{u}_0 \mathbf{u}_1 \cdots \mathbf{u}_{n-1}) = \sum_{i=1}^{n} w(\mathbf{u}_i)$, where $\mathbf{u}_i \in GF(2)^\tau$. The space of all binary vectors of length τn with the distance $d(\mathbf{x}, \mathbf{y}) = w_\tau(\mathbf{x} - \mathbf{y})$ is called the *ordered* Hamming space and is denoted by $H_2^{\tau,n}$. The space $H_2^{\tau,n}$ differs from the ordinary Hamming space $H_2^{\tau n}$ by the fact that on the set $GF(2)^{\tau n}$ the ordered weight $w_\tau(\mathbf{x})$ instead of the Hamming weight $w_H(\mathbf{x})$ is considered. For $\tau = 1$ these spaces coincide. Note that $w_H(\mathbf{x}) \le w_\tau(\mathbf{x})$ for any $\mathbf{x} \in GF(2)^{\tau n}$; we call $\mathbf{x} \in GF(2)^{\tau n}$ *complete* if $w_H(\mathbf{x}) = w_\tau(\mathbf{x})$. For example, for $\tau = 2$, $n = 4$, and $\mathbf{x} = 00011011$, we have $w_H(\mathbf{x}) = 4$, $w_2(\mathbf{x}) = 0+2+1+2 = 5$, and therefore $\mathbf{x}$ is not complete. On the other hand, for example the word 00111011 is complete.

Consider a binary matrix (code) C of size $2^k \times N$ with columns $\mathbf{A}_1, \ldots, \mathbf{A}_N$. We say that the columns $\mathbf{A}_{i_1}, \ldots, \mathbf{A}_{i_t}$ are *uniformly distributed* if each of the 2^t possible binary rows occurs 2^{k-t} times in the submatrix formed by these columns. Every subset $A = \{\mathbf{A}_{i_1}, \ldots, \mathbf{A}_{i_t}\}$ is characterized by the *indicator* binary vector $\mathbf{x}(A)$ of length N with ones in the positions $i_1, \ldots, i_t$. A number of combinatorial properties of C can be defined in terms of restrictions to subsets A of columns which must be uniformly distributed. The classical notion of an (N,k) *orthogonal array* of strength τ (shortly $\mathrm{OA}(\tau,k,N)$) introduced by Bose [1] requires that all subsets A which satisfy the inequalities $1 \le w_H(\mathbf{x}(A)) \le \tau$ must be uniformly distributed. In [6], one of the authors used the definition of *split orthogonal arrays* which is connected with other restrictions to subsets of columns subject to be uniformly distributed. The combinatorial interpretation of (n,k) hypercubic τ-designs found in [4], [7] can be rephrased that, for $N = \tau n$, all subsets A which satisfy the inequalities $1 \le w_\tau(\mathbf{x}(A)) \le \tau$ must be uniformly distributed. Such matrices of size $2^k \times \tau n$ are often called *ordered orthogonal arrays* of strength τ (shortly $\mathrm{OOA}(\tau,k,n)$.) Note that if a set A of columns is uniformly distributed, then this is also the case for any non-empty subset of A. Therefore, for the definitions of OA and OOA of strength τ, it is sufficient to require that this property is satisfied for sets A such that $w_H(\mathbf{x}(A)) = \tau$ and $w_H(\mathbf{x}(A)) = w_\tau(\mathbf{x}(A)) = \tau$, respectively. We call a subset A of the set of $N = \tau n$ columns *complete* if $w_H(\mathbf{x}(A)) = w_\tau(\mathbf{x}(A)) = \tau$.

In the case of *linear* codes the columns $\mathbf{A}_{i_1}, \ldots, \mathbf{A}_{i_t}$ are uniformly distributed if and only if they are linearly independent. Therefore, consideration of dual codes shows that the equivalence of (n,k) hypercubic τ-designs and $\mathrm{OOA}(\tau,k,n)$ can be extended to linear codes in $H_2^{\tau,n}$ with minimal ordered distance $\tau+1$. As a consequence one can use the Hamming bound for the size of such a code and obtain the generalized Rao bound [12] that shows that the size of a hypercubic τ-design and OOA of strength τ cannot be less than the size of a metric ball in $H_2^{\tau,n}$ of radius $\frac{\tau}{2}$. Martin and Stinson [7] proved that this bound is valid in the non-linear case and refined it for the case of odd τ. In [8] they investigated the space $H_2^{\tau,n}$ as an association scheme and OOA as codes in $H_2^{\tau,n}$ with dual distance $\tau+1$. Thus, it turned out that the problem of constructing hypercubic τ-designs or $(k-\tau,k,n)$-nets lies in the course of main problems of coding theory to construct a d-code of maximum size and τ-design of minimum size applied to the metric space $H_2^{\tau,n}$.

The matrix of an OOA(τ,k,n) consists of n successive groups of τ columns and from the definition of OOA of strength τ it follows that the first columns of these groups form an OA(τ,k,n). Therefore, it is natural for the construction of linear OOA(τ,k,n) to use the check matrices of known linear $[n,n-k]$ codes with minimal Hamming distance $\tau+1$ appending every column by a group of $\tau-1$ columns. This method was applied to construct minimum OOA of strength 2 and 3 from corresponding OA. Edel and Bierbrauer [2] constructed OOA's of strength 4 from OA's of strength 4 without increasing their sizes. They in fact used check matrices of some reversible codes with minimum distance 5 and a construction based on a tower of fields $GF(2), GF(2^m), GF(2^{2m}), GF(2^{4m})$. In this paper we propose a construction of OOA$(4,2m,2^m-1)$ from OA$(4,2m,2^m-1)$ which are dual of double-error-correcting BCH $[2^m-1, 2^m-1-2m]$ codes. Moreover, we use these codes to construct OOA$(5,2m+2,2^m-1)$. These OOA of strength 5 are half the size of the OOA obtained by the construction proposed in [5].

2 Constructing Linear OOA from Linear OA

We consider matrices with columns formed by binary vectors

$$\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_N. \tag{1}$$

We call a subset A of these columns a *τ-set* if $|A|=\tau$ or, equivalently, $w_H(\mathbf{x}(A))=\tau$ where $\mathbf{x}(A)\in GF(2)^N$ is the indicator vector of the set A. As we noted in the introduction, an *orthogonal array* OA(τ,k,n) (or τ-design) can be defined as a binary $2^k\times n$ matrix such that in any τ-set of columns, each possible τ-tuple occurs in exactly $2^{k-\tau}$ rows of those columns. A *linear* τ-design can be characterized as an $[n,k]$ code C generated by a $k\times n$ matrix G such that any set of τ columns from G are linearly independent.

To define and investigate ordered orthogonal arrays of strength τ for $N=n\tau$, it is suitable to split the columns into n groups of τ columns each and represent (1) as follows:

$$\mathbf{A}_{1,1},\ldots,\mathbf{A}_{1,\tau},\mathbf{A}_{2,1},\ldots,\mathbf{A}_{2,\tau},\ldots,\mathbf{A}_{n,1},\ldots,\mathbf{A}_{n,\tau}. \tag{2}$$

If a τ-set A of (2) is complete (i.e., $w_H(\mathbf{x}(A)) = w_\tau(\mathbf{x}(A)) = \tau$), then A contains the first $\tau_i \geq 0$, say, columns of group i for $i = 1, ..., n$, and we have a corresponding ordered partition

$$\tau_1 + \tau_2 + \cdots + \tau_n = \tau. \tag{3}$$

On the other hand, for any (ordered) partition (3) into nonnegative integers there is a corresponding complete τ-set. For a partition (3), consider the vector $(n_1, ..., n_l)$ where l is the number of groups with $\tau_i > 0$ and the components are the cardinalities of these groups arranged in decreasing order. The vector $(n_1, ..., n_l)$ is called the *type* of the complete τ-set. The number of types only depends on τ, not on the the number of columns. For example, there are 5 types of complete 4-sets: (1,1,1,1), (2,1,1), (2,2), (3,1), and (4).

An ordered orthogonal array $\mathrm{OOA}(\tau, k, n)$ is a binary $2^k \times n\tau$ matrix with the property that for each complete τ-set of columns, each possible τ-tuple occurs in exactly $2^{k-\tau}$ rows of those columns. A *linear* $\mathrm{OOA}(\tau, k, n)$ can be characterized as an $[n\tau, k]$ code C generated by a $k \times n\tau$ matrix G such that any complete τ-set of columns from G are linearly independent.

Note that the matrix consisting of the first column from each group of an $\mathrm{OOA}(\tau, k, n)$ is an $\mathrm{OA}(\tau, k, n)$. On the other hand, if for the construction of an $\mathrm{OOA}(\tau, k, n)$ one uses the columns of an $\mathrm{OA}(\tau, k, n)$ as first columns of the n groups, then all complete τ-sets of type $(1, 1, ..., 1)$ will be linearly independent. In [5] the following simple construction of a linear $\mathrm{OOA}(2s, k, n')$ with $n' = \lfloor \frac{n}{s} \rfloor$ from a linear $\mathrm{OA}(2s, k, n)$ and construction of a linear $\mathrm{OOA}(2s + 1, k, n')$ with $n' = \lfloor \frac{n-1}{s} \rfloor$ from a linear $\mathrm{OA}(2s + 1, k, n)$ were proposed which use similar arguments. Since $n \geq sn'$, $\mathrm{OA}(2s, k, n)$ contains sn' columns $\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_{sn'}$, any $2s$ of which are linearly independent. We define the first group in (2) as follows:

$$(\mathbf{A}_{1,1}, \ldots, \mathbf{A}_{1,2s}) = (\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_s, \mathbf{B}_{2s}, \mathbf{B}_{2s-1}, \ldots, \mathbf{B}_{s+1}),$$

and for $i = 2, ..., n'$, we define

$$(\mathbf{A}_{i,1}, \ldots, \mathbf{A}_{i,2s}) = (\mathbf{B}_{s(i-1)+1}, \mathbf{B}_{s(i-1)+2}, \ldots, \mathbf{B}_{si}, \mathbf{B}_s, \mathbf{B}_{s-1}, \ldots, \mathbf{B}_1).$$

Similarly, in the case $\tau = 2s + 1$, the $\mathrm{OA}(2s + 1, k, n)$ contains the $1 + sn'$ columns $\mathbf{B}_0, \mathbf{B}_1, \ldots, \mathbf{B}_{sn'}$, any $2s + 1$ of which are linearly independent. The construction above is modified by inserting the column $\mathbf{B}_0$ in the middle of each block:

$$(\mathbf{A}_{1,1}, \ldots, \mathbf{A}_{1,2s+1}) = (\mathbf{B}_1, \ldots, \mathbf{B}_s, \mathbf{B}_0, \mathbf{B}_{2s}, \ldots, \mathbf{B}_{s+1}),$$

$$(\mathbf{A}_{i,1},\ldots,\mathbf{A}_{i,2s+1}) = (\mathbf{B}_{s(i-1)+1},\ldots,\mathbf{B}_{si},\mathbf{B}_0,\mathbf{B}_s,\ldots,\mathbf{B}_1).$$

In this construction any column in (2) is a column of $\mathrm{OA}(\tau,k,n)$ and it is easy to see that any complete τ-set of columns (2) consist of τ distinct columns of $\mathrm{OA}(\tau,k,n)$. This substantiates the construction. Using in this construction the $\mathrm{OA}(2s,sm,2^m-1)$ and $\mathrm{OA}(2s+1,sm+1,2^m)$ which are dual to primitive s-error-correcting BCH codes and to their extensions, we get optimal constructions for $\tau \le 3$, but constructions which are not optimal for $\tau \ge 4$. In particular, it gives $\mathrm{OOA}(4,2m+2,2^m-1)$ and $\mathrm{OOA}(5,2m+3,2^m-1)$. In [2], Edel and Bierbrauer used primitive double-error-correcting BCH codes to construct $\mathrm{OOA}(4,2m,2^m-2)$. In this paper we will describe constructions for $\mathrm{OOA}(4,2m,2^m-1)$ and $\mathrm{OOA}(5,2m+2,2^m-1)$.

3 Construction of Linear Ordered 4-Designs

Let C be a (binary) linear $[n,n-k,\tau+1]$ code C with vectors

$$\mathbf{B}_1,\mathbf{B}_2,\ldots,\mathbf{B}_n \tag{4}$$

of length k as columns of its check matrix H. The matrix H is generator matrix of an $\mathrm{OA}(\tau,k,n)$. To construct the columns (2) of an OOA with the help of (4) we use a method where each $\mathbf{A}_{i,j}$ is a linear combination of the columns (4). In this case any linear combination of the columns (2) is a linear combination of the columns (4), and the question about linear independence of complete τ-sets of columns (2) is reduced to the question of C not containing some particular words.

To simplify, we describe this method for the class of cyclic codes and $\tau = 4$. The vectors $\mathbf{c} = (c_1,\ldots,c_n) \in GF(2)^n$ we shall also represent as words $\mathbf{c} = c_1\cdots c_n$ and polynomials $\mathbf{c}(x) = \sum_{i=1}^n c_i x^{i-1}$ when convenient. By definition, $\mathbf{c} \in C$ if and only if $\sum_{i=1}^n c_i\mathbf{B}_i = \mathbf{0}$. Let

$$\mathbf{c}_j = (c_{j,1},\ldots,c_{j,n}), \quad j = 1,2,3,4, \tag{5}$$

be arbitrary vectors of $GF(2)^n$. For any linear cyclic $[n,n-k]$ code C with check matrix (4), denote by $C^{\perp}(\mathbf{c}_1,\mathbf{c}_2,\mathbf{c}_3,\mathbf{c}_4)$ the $[4n,k]$ code D with generator matrix (2) where

$$\mathbf{A}_{i,j} = \sum_{h=1}^{n} c_{j,h-i+1}\mathbf{B}_h, \quad i = 1,...,n,\ j = 1,2,3,4. \tag{6}$$

Here and in the following subscripts are taken modulo n.

For $\mathbf{c} = (c_1, \ldots, c_n) \in GF(2)^n$, we denote its cyclic shift l steps to the right, i.e., $(c_{n-l+1}, \ldots, c_n, c_1, \ldots, c_{n-l})$, by $\mathbf{c}^{(l)}$. It is clear that if $\mathbf{c} \in GF(2)^n \setminus \{\mathbf{0}, \mathbf{1}\}$, then there exist positive integers r and a_i, b_i, $i = 1, ..., r$, such that $\mathbf{c}^{(l)} = 1^{a_1}0^{b_1} \cdots 1^{a_r}0^{b_r}$ for some l. In this case one says that $\mathbf{c}$ has r *runs* of lengths a_i, $i = 1, ..., r$. If $\mathbf{c}$ has r runs then $w_H(\mathbf{c} + \mathbf{c}^{(1)}) = 2r$ and hence a linear cyclic code with minimum distance $2r + 1$ cannot contain words with r or less runs.

Note that any relation

$$\sum_{i=1}^{n} \sum_{j=1}^{4} d_{i,j} \mathbf{A}_{i,j} = \mathbf{0} \tag{7}$$

where $d_{i,j} \in \{0, 1\}$ implies that the vector

$$\mathbf{y} = (y_1, \ldots, y_n) = \sum_{i=1}^{n} \sum_{j=1}^{4} d_{i,j} \mathbf{c}_j^{(i-1)} \tag{8}$$

belongs to C because

$$\sum_{h=1}^{n} y_h \mathbf{B}_h = \sum_{h=1}^{n} \sum_{i=1}^{n} \sum_{j=1}^{4} d_{i,j} c_{j,h-i+1} \mathbf{B}_h = \sum_{i=1}^{n} \sum_{j=1}^{4} d_{i,j} \mathbf{A}_{i,j} = \mathbf{0},$$

by (6). Since C is a cyclic code and hence $\mathbf{y}^{(l)} \in C$, (7) also implies that for any $l = 1, ..., n-1$,

$$\begin{aligned} \mathbf{0} &= \sum_{h=1}^{n} y_{h-l} \mathbf{B}_h = \sum_{h=1}^{n} \sum_{i=1}^{n} \sum_{j=1}^{4} d_{i,j} c_{j,h-i-l+1} \mathbf{B}_h \\ &= \sum_{i=1}^{n} \sum_{j=1}^{4} d_{i,j} \sum_{h=1}^{n} c_{j,h-i-l+1} \mathbf{B}_h = \sum_{i=1}^{n} \sum_{j=1}^{4} d_{i,j} \mathbf{A}_{i+l,j}. \end{aligned} \tag{9}$$

To investigate the codes $C^{\perp}(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4)$ we first note that if C is a linear cyclic code with minimum distance 5, then C does not contain words with 1 or 2 runs.

For any integer ν, $4 \leq \nu \leq n-3$, consider the following special case of (5):

$$\mathbf{c}_1 = 10^{n-1}, \ \mathbf{c}_2 = 01^{\nu}0^{n-\nu-1}, \ \mathbf{c}_3 = 01^{\nu-2}0^{n-\nu+1}, \ \mathbf{c}_4 = 010^{n-2}. \tag{10}$$

The corresponding polynomial representations of these code words are:

$$1, \ x\frac{x^{\nu}+1}{x+1}, \ x\frac{x^{\nu-2}+1}{x+1}, \ x.$$

In this case, we will write $C^{\perp}(\nu)$ instead of $C^{\perp}(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4)$.

Lemma 1 *Let C be a binary linear cyclic $[n, n-k, 5]$ code and let $4 \leq \nu \leq n-3$. Moreover, if C contains $\mathbf{1}$, then we also assume that $2\nu \notin \{n-2, n-1, n\}$. Then $C^{\perp}(\nu)$ is $OOA(4, k, n)$ if C does not contain any polynomials of the form*

$$a + x\frac{x^{\nu}+1}{x+1} + x^i + x^j = \frac{x^{\nu+1}+x^{1-a}}{x+1} + x^i + x^j \tag{11}$$

where $a \in \{0, 1\}$ and $\nu + 1 < i < j \leq n$.

Proof. We will show that under these conditions all complete 4-sets of columns of the generator matrix (2) are linearly independent. In the proof, for any complete 4-set A with the indicator vector

$$\mathbf{x}(A) = (d_{1,1}, ..., d_{1,4}, ..., d_{n,1}, ..., d_{n,4}) \in GF(2)^{4n}$$

where $w_H(\mathbf{x}(A)) = w_4(\mathbf{x}(A)) = 4$, we verify that (7) implies that the corresponding vector $\mathbf{y} \in C$ given by (8) equals $\mathbf{0}$. There are five types of complete 4-sets (5 partitions of 4) and we treat them one at the time. Since (7) implies (9), we can assume without loss of generality that, for any type, the first group of 4 columns contains the maximal number of columns of the complete 4-set under consideration.

Type (1,1,1,1). Since $\mathbf{A}_{i,1} = \mathbf{B}_i$ for all i, by (6) and (10), any four $\mathbf{A}_{i,1}$ are linearly independent.

Type (2,1,1). We can rewrite (7) as

$$d_{1,1}\mathbf{A}_{1,1} + d_{1,2}\mathbf{A}_{1,2} + d_{i,1}\mathbf{A}_{i,1} + d_{j,1}\mathbf{A}_{j,1} = \mathbf{0}$$

where $1 < i < j \leq n$. If $d_{1,2} = 0$, this is a special case of type (1,1,1,1). Suppose $d_{1,2} = 1$. If at least one of $d_{i,1}$ and $d_{j,1}$ is zero, then according to (10) the vector $\mathbf{y} \in C$ given by (8) is the sum of the vector $d_{1,1}\mathbf{c}_1 + \mathbf{c}_2$ which has a single run of length ν or $\nu+1$ and a vector of weight at most 1. That is impossible since C has minimum distance 5. Finally, if $d_{1,2} = d_{i,1} = d_{j,1} = 1$,

then the polynomial representation of $\mathbf{y}$ is of the form (11) with $a = d_{1,1}$, contradicting the assumptions of the lemma.
Type (2,2). Suppose that

$$d_{1,1}\mathbf{A}_{1,1} + d_{1,2}\mathbf{A}_{1,2} + d_{i,1}\mathbf{A}_{i,1} + d_{i,2}\mathbf{A}_{i,2} = 0$$

where $1 < i \leq n$. Similarly to the previous type, $\mathbf{y}$ is the sum of two vectors, each having at most one run. Hence $\mathbf{y}$ has at most 2 runs or equals $\mathbf{1}$, which is possible only if $2\nu \in \{n-2, n-1, n\}$. Therefore, $\mathbf{y} = \mathbf{0}$.
Types (3,1) and (4). We note that since $\mathbf{A}_{1,4} = \mathbf{A}_{2,1}$, a complete 4-set of type (4) is a special case of a complete 4-set of type (3,1). Hence it is sufficient to consider type (3,1). Suppose that

$$d_{1,1}\mathbf{A}_{1,1} + d_{1,2}\mathbf{A}_{1,2} + d_{1,3}\mathbf{A}_{1,3} + d_{i,1}\mathbf{A}_{i,1} = 0$$

where $1 < i \leq n$. If $d_{1,2} = d_{1,3}$, then the vector $\mathbf{y}$ is the sum of two vectors $d_{1,2}\mathbf{c}_2 + d_{1,3}\mathbf{c}_3$ and $d_{1,1}\mathbf{c}_1 + d_{i,1}\mathbf{c}_1^{(i-1)}$ each of which has Hamming weight at most 2. Hence the Hamming weight of $\mathbf{y}$ is at most 4 and so $\mathbf{y} = \mathbf{0}$. If $d_{1,2} \neq d_{1,3}$, then the vector $\mathbf{y}$ is the sum of two vectors $d_{1,1}\mathbf{c}_1 + d_{1,2}\mathbf{c}_2 + d_{1,3}\mathbf{c}_3$ and $d_{i,1}\mathbf{c}_1^{(i-1)}$. The first vector has exactly one run, the second vector does not coincide with the first one and has at most one run. This is not possible. □

Now we apply Lemma 1 to double-error correcting BCH codes and show that the required condition can be fulfilled for some restriction on the selection of an element $\alpha \in GF(2^m)$. Let $n \geq 7$ be an odd integer, and let m be the multiplicative order of 2 modulo n, that is, the least positive integer such that $2^m - 1$ is divisible by n. Let $\alpha \in GF(2^m)$ have order n, that is $\alpha^n = 1$ and n is the smallest positive integer with this property. Consider the linear cyclic $[n, n-2m]$ code C with check matrix formed by the columns (4) where $\mathbf{B}_i = (\alpha^i, \alpha^{3i})$, $i = 1, \ldots, n$. C has minimum distance at least 5 by the BCH bound. We investigate first the code $C^{\perp}(\nu)$ for $\nu = \frac{n+1}{2}$ and will return to other values of ν later. We use Tr to denote the trace function $GF(2^m) \to GF(2)$ defined by

$$\mathrm{Tr}(z) = \sum_{i=0}^{m-1} z^{2^i}.$$

Theorem 1 *For $m \geq 3$ and odd $n \geq 2m+1$, let $\alpha \in GF(2^m)$ of order n satisfy the conditions*

$$\mathrm{Tr}\left(\frac{\alpha}{\alpha^2+\alpha+1}\right) = \mathrm{Tr}\left(\frac{\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2}{(\alpha^2+\alpha+1)^4}\right) = 1. \tag{12}$$

If C is the $[n, n-2m]$ BCH code described above, then the code $C^{\perp}(\frac{n+1}{2})$ is $OOA(4, 2m, n)$.

Proof. First note that for odd $n \geq 2m+1 \geq 7$ and $\nu = \frac{n+1}{2}$ both the inequalities $4 \leq \nu \leq n-3$ hold. Since α and α^3 are roots of the generator polynomial of the cyclic code C, this is also true for α^2 and α^6. Therefore, if the polynomial (11) belongs to C, then the system

$$\begin{cases} x+y &= u \\ x^3+y^3 &= v \end{cases}$$

where

$$u = \frac{\alpha^{2(\nu+1)}+\alpha^{2(1-a)}}{\alpha^2+1}, \quad v = \frac{\alpha^{6(\nu+1)}+\alpha^{6(1-a)}}{\alpha^6+1} \tag{13}$$

has the solution $x = \alpha^{2i}$ and $y = \alpha^{2j}$ in $GF(2^m)$. Since x and y are distinct, we have $u \neq 0$. Combining these two equations we get

$$v = x^3 + (x+u)^3 = ux^2 + u^2x + u^3,$$

and so x is root of the equation

$$x^2 + ux + \frac{u^3+v}{u} = 0. \tag{14}$$

It is known that if an equation $x^2+ux+w=0$, where $u, w \in GF(2^m)$, $u \neq 0$, has solutions in $GF(2^m)$, then $\mathrm{Tr}(w/u^2) = 0$. Hence by (14)

$$\mathrm{Tr}\left(\frac{u^3+v}{u^3}\right) = 0.$$

Due to (13) and the relation $\alpha^{2\nu} = \alpha$, this is equivalent to

$$\mathrm{Tr}\left(\frac{\alpha}{\alpha^2+\alpha+1}\right) = 0 \quad \text{and} \quad \mathrm{Tr}\left(\frac{\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2}{(\alpha^2+\alpha+1)^4}\right) = 0,$$

for $a = 0$ and $a = 1$, respectively, and so contradicts the conditions of the theorem. $\square$

Other choices of ν give results similar to Theorem 1 but with other trace conditions. We state a couple of them without proof (note that $\nu = \frac{n-1}{2}$ is not possible since $2\nu = n - 1$ and C contains $\mathbf{1}$):

$C^{\perp}(\frac{n+3}{2})$ is OOA$(4, 2m, n)$ if α satisfies the conditions

$$\mathrm{Tr}\left(\frac{\alpha^2(\alpha+1)^3(\alpha^5+1)}{(\alpha^3+1)^4}\right) = \mathrm{Tr}\left(\frac{\alpha^2(\alpha+1)^2(\alpha^7+1)}{(\alpha^3+1)(\alpha^5+1)^2}\right) = 1.$$

$C^{\perp}(\frac{n+5}{2})$ is OOA$(4, 2m, n)$ if α satisfies the conditions

$$\begin{aligned} &\mathrm{Tr}\left(\frac{\alpha^2(\alpha+1)^2(\alpha^7+1)}{(\alpha^3+1)(\alpha^5+1)^2}\right) \\ = \quad &\mathrm{Tr}\left(\frac{\alpha^2(\alpha+1)^3(\alpha^{10}+\alpha^9+\alpha^8+\alpha^5+\alpha^2+\alpha+1)}{(\alpha^3+1)(\alpha^7+1)^2}\right) = 1. \end{aligned}$$

Now we apply Lemma 1 to some BCH codes with minimum distance 6. Let m be even and let $\alpha \in GF(2^m)$ of order n dividing $2^{m/2}+1$. Consider the linear cyclic $[n, n-m-1]$ code C_1 with α and 1 as zeros of the generator polynomial. Since $\alpha^{2^{m/2}} = \alpha^{-1}$, the generator polynomial has zeroes α^{-2}, α^{-1}, 1, α, α^2. By the BCH bound, the minimum distance of the code is at least 6. A check matrix of C_1 is formed by the columns (4) where $\mathbf{B}_i = (\alpha^i, 1)$, $i = 1, \ldots, n$ have length $m+1$. Since C_1 does not contain $\mathbf{1} \in GF(2)^n$ we can apply Lemma 1 for $\nu = \frac{n-1}{2}$.

Theorem 2 *Let m be even, $n \geq m+2$ such that n divides $2^{m/2}+1$, and let C_1 be the $[n, n-m-1, 6]$ BCH code described above, having $\alpha \in GF(2^m)$ of order n as root of the generator polynomial. If*

$$\mathrm{Tr}(\alpha) = 0, \tag{15}$$

then the code $C_1^{\perp}(\frac{n-1}{2})$ is OOA$(4, m, n)$.

Proof. Suppose that C_1 contains a polynomial (11). Since α and α^{-1} are roots of the generator polynomial of C_1, α satisfies the equations

$$\alpha^i + \alpha^j = \alpha^{1-a}\frac{1+\alpha^{\nu+a}}{1+\alpha},$$

$$\alpha^{-i}+\alpha^{-j}=\alpha^{-(1-a)}\frac{1+\alpha^{-(\nu+a)}}{1+\alpha^{-1}}=\alpha^{-\nu}\frac{1+\alpha^{\nu+a}}{1+\alpha}.$$

Since $\alpha^i+\alpha^j=\alpha^{i+j}(\alpha^{-i}+\alpha^{-j})$ we have $\alpha^{i+j}=\alpha^{\nu+1-a}$ and

$$i+j\equiv\nu+1-a \pmod n. \tag{16}$$

From $\nu=\frac{n-1}{2}$ and $\alpha^{2\nu}=\alpha^{-1}$ we get

$$2i+a+2j+a\equiv 1 \pmod n, \tag{17}$$

$$\alpha^{2i}+\alpha^{2j}=\alpha^{2-2a}\frac{1+\alpha^{-1+2a}}{1+\alpha^2}=\alpha\frac{1+\alpha^{1-2a}}{1+\alpha^2},$$

and hence for any $a\in\{0,1\}$ we have,

$$\alpha^{2i+a}+\alpha^{2j+a}=\alpha\frac{\alpha^a+\alpha^{1-a}}{1+\alpha^2}=\frac{\alpha}{1+\alpha}. \tag{18}$$

Putting $x=\alpha^{2i+a}$ and noting that $\alpha^{2j+a}=\alpha x^{-1}$, by (17), one can rewrite (18) as

$$x^2+ux+w=0 \quad \text{where} \quad u=\frac{\alpha}{1+\alpha},\ w=\alpha. \tag{19}$$

Next we show by induction that for $i\geq 1$ we have

$$x^{2^i}=u^{2^i-1}\left(x+u\sum_{h=1}^{i}\left(\frac{w}{u^2}\right)^{2^{h-1}}\right). \tag{20}$$

This is true for $i=1$ by (19). Suppose that (20) is true for i. Then

$$\begin{aligned}
x^{2^{i+1}} &= u^{2^{i+1}-2}\left(x^2+u^2\sum_{h=1}^{i}\left(\frac{w}{u^2}\right)^{2^h}\right)\\
&= u^{2^{i+1}-2}\left(ux+w+u^2\sum_{h=1}^{i}\left(\frac{w}{u^2}\right)^{2^h}\right)\\
&= u^{2^{i+1}-1}\left(x+u\sum_{h=0}^{i}\left(\frac{w}{u^2}\right)^{2^h}\right)\\
&= u^{2^{i+1}-1}\left(x+u\sum_{h=1}^{i+1}\left(\frac{w}{u^2}\right)^{2^{h-1}}\right).
\end{aligned}$$

This completes the induction. Since $n \mid 2^{m/2}+1$, we have $x^{2^{m/2}+1} = 1$. Hence $i = m/2$ in (20) gives

$$x^2 + u \sum_{h=1}^{m/2} \left(\frac{w}{u^2}\right)^{2^{h-1}} x + u^{-2^{m/2}+1} = 0. \tag{21}$$

We have

$$\begin{aligned} u^{-2^{m/2}+1} &= \frac{\alpha}{1+\alpha}\left(1+\frac{1}{\alpha}\right)^{2^{m/2}} = \frac{\alpha}{1+\alpha}\left(1+\frac{1}{\alpha^{2^{m/2}}}\right) \\ &= \frac{\alpha}{1+\alpha}\left(1+\frac{1}{\alpha^{-1}}\right) = \alpha = w \end{aligned}$$

and

$$\sum_{h=1}^{m/2} \left(\frac{w}{u^2}\right)^{2^{h-1}} = \sum_{h=1}^{m/2} \left(\alpha+\alpha^{-1}\right)^{2^{h-1}} = \sum_{h=1}^{m} \alpha^{2^{h-1}} = \mathrm{Tr}(\alpha).$$

Hence, since $u \neq 0$, (19) and (21) are the same equation and so $\mathrm{Tr}(\alpha) = 1$, contradicting the condition (15). $\square$

4 Satisfying the Trace Conditions

For Theorem 1 to apply for particular n and m, it is necessary to have an $\alpha \in GF(2^m)$ of order n satisfying the trace conditions (12). The question when such an α exists seems to be hard to answer in general. We first give a table of the number of primitive α (that is, $n = 2^m - 1$) satisfying (12) for $m \leq 16$.

m	number	m	number	m	number	m	number	m	number
3	0	6	12	9	126	12	480	15	6690
4	8	7	56	10	140	13	2080	16	8480
5	0	8	32	11	440	14	2520		

We see that for $6 \leq m \leq 16$ primitive α satisfying (12) exist. The number of such α increases exponentially with m and it seems reasonable to expect this to be the case also for larger m.

For $m \leq 16$ we have also checked for $2m+1 \leq n \leq 2^m - 1$ if there exists an α of order n satisfying (12). It turn out that for $m \geq 6$ this is the case if n is sufficiently large. More precisely, there is a smallest order $n(m)$ such that for all orders $n \geq n(m)$, such α exist, and for all lower orders such α do not exist. The values of $n(m)$ are given in the following table. We have also included the largest order less than $n(m)$, denoted by $n'(m)$, that is, the largest order for which no α exists (if $n'(m) < 2m + 1$ it is included in brackets).

m	$n'(m)$	$n(m)$	m	$n'(m)$	$n(m)$	m	$n'(m)$	$n(m)$	m	$n'(m)$	$n(m)$
6	21	63	9	[7]	73	12	65	91	15	31	151
7	[1]	127	10	93	341	13	[1]	8191	16	257	771
8	51	85	11	89	2047	14	129	381			

If these exists such an $n(m)$ for all $m \geq 6$ is an open question.

It appears to be hard to prove results about when α of a given order exists or not. However, we will give some partial results. The following lemma is a special case of Theorem 2 in [9].

Lemma 2 *Let $\bar{F}$ denote the algebraic closure of $GF(2^m)$. Let $f(z)$, $g(z) \in GF(2^m)[z]$, where $\deg f < r = \deg g$ and $g(z)$ is a polynomial with t distinct zeros in $\bar{F}$. If $\frac{f(z)}{g(z)} \neq h(z)^2 + h(z)$ for any rational function $h \in \bar{F}(z)$, then*

$$\Big| \sum_{z \in L} (-1)^{\mathrm{Tr}(\frac{f(z)}{g(z)})} \Big| \leq (t + r - 2)\sqrt{2^m} + 1$$

where L consists of all elements of $GF(2^m)$ except the zeros of $g(z)$.

Theorem 3 *Let L consist of all elements of $GF(2^m)$ except the zeros of $z^2 + z + 1$. Let N_m denote the number of $z \in L$ that satisfies*

$$\mathrm{Tr}\left(\frac{z}{z^2 + z + 1}\right) = 1 \quad \textit{and} \quad \mathrm{Tr}\left(\frac{z^6 + z^5 + z^4 + z^3 + z^2}{(z^2 + z + 1)^4}\right) = 1.$$

Then

$$N_m \geq \frac{2^m - 5 - 18\sqrt{2^m}}{4}.$$

Proof. We have that

$$4N_m = \sum_{z \in L} \left(1 - (-1)^{\mathrm{Tr}(\frac{z}{z^2+z+1})}\right) \left(1 - (-1)^{\mathrm{Tr}(\frac{z^6+z^5+z^4+z^3+z^2}{(z^2+z+1)^4})}\right)$$

$$
\begin{aligned}
&= |L| - \sum_{z\in L}(-1)^{\mathrm{Tr}(\frac{z}{z^2+z+1})} - \sum_{z\in L}(-1)^{\mathrm{Tr}(\frac{z^6+z^5+z^4+z^3+z^2}{(z^2+z+1)^4})} \\
&\quad + \sum_{z\in L}(-1)^{\mathrm{Tr}(\frac{z}{z^2+z+1}+\frac{z^6+z^5+z^4+z^3+z^2}{(z^2+z+1)^4})} \\
&= |L| - \sum_{z\in L}(-1)^{\mathrm{Tr}(\frac{z}{z^2+z+1})} - \sum_{z\in L}(-1)^{\mathrm{Tr}(\frac{z^6+z^5+z^4+z^3+z^2}{(z^2+z+1)^4})} \\
&\quad + \sum_{z\in L}(-1)^{\mathrm{Tr}(\frac{z^7+z^5+z^3+z}{(z^2+z+1)^4})}.
\end{aligned}
$$

First we show that there is no rational $h(z) \in \bar{F}(z)$ such that

$$h(z)^2 + h(z) = \frac{z}{z^2+z+1}.$$

Suppose there is a solution $h(z) = \frac{f(z)}{g(z)}$, where we can assume without loss of generality that $\gcd(f(z), g(z)) = 1$. We obtain,

$$zg(z)^2 = (z^2+z+1)f(z)(f(z)+g(z)).$$

Let $z^2+z+1 = (z+\alpha)(z+\beta)$. Then it follows that $z+\alpha$ divides $g(z)$. Further, $z+\alpha$ does not divide $f(z)$ or $f(z)+g(z)$ since $\gcd(f(z), g(z)) = 1$. This leads to a contradiction since the left hand side is divisible with $z+\alpha$ to an even power while the right hand side is exactly divisible with $z+\alpha$.

We next show that there is no rational solution of

$$h(z)^2 + h(z) = \frac{z^6+z^5+z^4+z^3+z^2}{(z^2+z+1)^4}.$$

Suppose there is a solution $h(z) = \frac{f(z)}{g(z)}$, where $\gcd(f(z), g(z)) = 1$. Then,

$$z^2(z^4+z^3+z^2+z+1)g(z)^2 = (z^2+z+1)^4 f(z)(f(z)+g(z)).$$

We have, $\gcd(f(z), f(z)+g(z)) = 1$ and $\gcd(z^2(z^4+z^3+z^2+z+1), (z^2+z+1)^4) = 1$ since $\gcd(z^4+z^3+z^2+z+1, z^2+z+1) = 1$. It follows that

$$g(z) = (z^2+z+1)^2$$

and

$$f(z)(f(z)+z^4+z^2+1) = z^2(z^4+z^3+z^2+z+1).$$

It follows that $f(z)$ has degree at most 4. Let $f(z) = f_0 + f_1 z + f_2 z^2 + f_3 z^3 + f_4 z^4$. Comparing coefficients of degree 7 and degree 1 on each side implies $f_3 = 0$ and $f_1 = 0$ respectively. However, now a comparison of the coefficients of degree 3 leads to a contradiction.

Finally, we show that there is no rational solution of the equation

$$h(z)^2 + h(z) = \frac{z^7 + z^5 + z^3 + z}{(z^2 + z + 1)^4}.$$

Suppose there is a solution $h(z) = \frac{f(z)}{g(z)}$, where $\gcd(f(z), g(z)) = 1$. Then,

$$(z^7 + z^5 + z^3 + z)g(z)^2 = (z^2 + z + 1)^4 f(z)(f(z) + g(z)).$$

It follows as above that

$$g(z) = (z^2 + z + 1)^2$$

and

$$f(z)(f(z) + z^4 + z^2 + 1) = z^7 + z^5 + z^3 + z.$$

It follows that $f(z)$ has degree at most 4. Let $f(z) = f_0 + f_1 z + f_2 z^2 + f_3 z^3 + f_4 z^4$. Comparing coefficients of degree 7 and degree 1 on each side implies $f_3 = 1$ and $f_1 = 1$ respectively. Comparing coefficients of degree 5 implies $f_1 + f_3 = 1$, a contradiction.

By Lemma 2, we obtain

$$4N_m \geq |L| - (2\sqrt{2^m} + 1) - (8\sqrt{2^m} + 1) - (8\sqrt{2^m} + 1) \geq 2^m - 5 - 18\sqrt{2^m}$$

since $|L| = 2^m - 2$ if m is even and $|L| = 2^m$ otherwise. $\square$

Theorem 3 estimates the number of α *of all orders* satisfying (12). For some cases we can say something about primitive α, that is α of order $n = 2^m - 1$.

Corollary 1 *The number of primitive $\alpha \in GF(2^m)$ satisfying (12) is lower bounded by*

$$\varphi(n) - \frac{3n + 4 + 18\sqrt{n+1}}{4},$$

where $n = 2^m - 1$ and φ is Euler's totient function.

Proof. Let $\beta \in GF(2^m)$ be primitive. Then

$$GF(2^m)^* = GF(2^m) \setminus \{0\} = \{\beta^i \mid 0 \le i \le n-1\}.$$

The set $GF(2^m)^*$ contains n elements and $\varphi(n)$ of these are primitive (have order n). By Theorem 3, at least $\frac{n-4-18\sqrt{n+1}}{4}$ of the elements satisfy (12). Hence, the number of elements in $GF(2^m)^*$ of order n which satisfy (12) is at least

$$\varphi(n) + \frac{n-4-18\sqrt{n+1}}{4} - n = \varphi(n) - \frac{3n+4+18\sqrt{n+1}}{4}.$$

□

The lower bound is useless if it is negative. It is easy to see that this is the case for all even m. However, for most odd $m \ge 11$ of reasonable size it is positive and hence proves that primitive α satisfying (12) exist. In particular, this is the case for all odd m such that $11 \le m \le 135$. An example of an odd $m > 11$ where the bound is negative is $m = 3^2 \cdot 5 \cdot 7 \cdot 11 = 3465$. We can show this without finding the complete factorization of $n = 2^{3465} - 1$. It is sufficient to show that the primes in the set $P = \{7, 23, 31, 71, 73, 89, 127, 151, 199\}$ all divide n; equivalently, that $\mathrm{ord}_p\, 2$ divides m for all $p \in P$ (here $\mathrm{ord}_p\, 2$ is the order of 2 modulo p). In the following table we list these orders.

p	7	23	31	71	73	89	127	151	199
$\mathrm{ord}_p\, 2$	3	11	5	25	9	11	7	15	99

We see that $\mathrm{ord}_p\, 2$ divides m for all $p \in P$. Hence

$$\varphi(n) = n \prod_{p|n} \frac{p-1}{p} \le n \prod_{p \in P} \frac{p-1}{p} \approx 0.748\, n$$

and so the bound of Corollary 1 is negative.

We next consider, for even m, $\alpha \in GF(2^m)$ of order $n = 2^{m/2}+1$ satisfying (15). The total number of $\alpha \in GF(2^m)$ of order n is $\varphi(n)$. In the following table we list $\varphi(n)$ and the number of $\alpha \in GF(2^m)$ of order n satisfying $\mathrm{Tr}(\alpha) = 0$ for $m \le 20$.

m	2	4	6	8	10	12	14	16	18	20
$\varphi(n)$	2	4	6	16	20	48	84	256	324	800
No. satisfying $\mathrm{Tr}(\alpha) = 0$	0	0	6	8	10	36	42	112	144	400

The number seems to grow exponentially with m. In the next lemma we give a bound which is similar to Corollary 1.

Lemma 3 *Let m be even. The number of $\alpha \in GF(2^m)$ of order $n = 2^{m/2}+1$ satisfying* $\mathrm{Tr}(\alpha) = 0$ *is lower bounded by*

$$\varphi(n) - \frac{n}{2} - \sqrt{n-1}.$$

Proof. Let $\beta \in GF(2^m)$ have order n. Consider the set

$$S = \{\beta^i \mid 0 \le i \le n-1\}.$$

The set S contains n elements and $\varphi(n)$ of these have order n. Theorem 6.6 in [3] implies that at least $\frac{n}{2} - \sqrt{n-1}$ of the elements of S have trace 0. Hence, the number of elements in S with order n and trace 0 is at least

$$\varphi(n) + \left(\frac{n}{2} - \sqrt{n-1}\right) - n = \varphi(n) - \frac{n}{2} - \sqrt{n-1}.$$

□

The lower bound is positive for all even m in the range $10 \le m \le 300$. We expect that there are values of m where the lower bound is negative, but they are probably quite large.

A computation also shows that for all even m, $6 \le m \le 20$ and all n such that $m+2 \le n \le 2^{m/2}+1$ and $n \mid 2^{m/2}+1$, there exist α satisfying (15). If this is true for all even $m \ge 6$ is an open question.

5 Construction of Hypercubic 5-Designs

We have considered a construction of hypercubic 4-designs from $[n, n-2m]$ double-error-correcting BCH codes. For this code n is an odd integer ($n \ge 3$) and m is the multiplicative order of 2 modulo n. The check matrix of this code is formed by columns (4) with $\mathbf{B}_i = (\alpha^i, \alpha^{3i})$, $i = 1, \ldots, n$ where $\alpha \in GF(2^m)$ is such that $\alpha^n = 1$ and n is the smallest positive integer with this property. Now we use this construction to obtain an OOA of strength 5 appending two additional rows to this check matrix.

Consider the following column vectors of length $2m+2$:

$$\mathbf{A}_i = (\alpha^i, \alpha^{3i}, 10), \mathbf{B}_i = (\alpha^i, (\alpha^{3i} + \alpha^i), 11), \mathbf{U} = (00\cdots010), \mathbf{V} = (00\cdots001).$$

Denote by D the $[5n, 2m+2]$ code whose generator matrix is formed by the column vectors (2) with $\tau = 5$ where

$$\mathbf{A}_{i,1} = \mathbf{A}_i,\ \mathbf{A}_{i,2} = \mathbf{B}_i,\ \mathbf{A}_{i,3} = \mathbf{U},\ \mathbf{A}_{i,4} = \mathbf{V},\ \mathbf{A}_{i,5} = \mathbf{A}_{i+1}.$$

Theorem 4 *The* $[5n, 2m+2]$ *code* D *is* $OOA(5, 2m+2, n)$.

Proof. We have to show that all complete 5-sets of columns are linearly independent. There are 7 types of such sets and we consider them one at the time.

Type (1,1,1,1,1). Suppose that

$$a_1\mathbf{A}_{i_1} + a_2\mathbf{A}_{i_2} + a_3\mathbf{A}_{i_3} + a_4\mathbf{A}_{i_4} + a_5\mathbf{A}_{i_5} = 0.$$

Then

$$a_1\alpha^{i_1} + a_2\alpha^{i_2} + a_3\alpha^{i_3} + a_4\alpha^{i_4} + a_5\alpha^{i_5} = 0, \tag{22}$$

$$a_1\alpha^{3i_1} + a_2\alpha^{3i_2} + a_3\alpha^{3i_3} + a_4\alpha^{3i_4} + a_5\alpha^{3i_5} = 0, \tag{23}$$

$$a_1 + a_2 + a_3 + a_4 + a_5 = 0.$$

From the last equation we see that $(a_1, a_2, a_3, a_4, a_5)$ has weight 0, 2, or 4. Since the BCH code has minimum distance 5, (22) and (23) implies that $(a_1, a_2, a_3, a_4, a_5) = (0, 0, 0, 0, 0)$.

Type (2,1,1,1). Suppose that

$$a_1\mathbf{A}_{i_1} + b\mathbf{B}_{i_1} + a_2\mathbf{A}_{i_2} + a_3\mathbf{A}_{i_3} + a_4\mathbf{A}_{i_4} = 0.$$

Then

$$\begin{aligned}
&a_1\alpha^{i_1} + b\alpha^{i_1} + a_2\alpha^{i_2} + a_3\alpha^{i_3} + a_4\alpha^{i_4} = 0,\\
&a_1\alpha^{3i_1} + b(\alpha^{3i_1} + \alpha^{i_1}) + a_2\alpha^{3i_2} + a_3\alpha^{3i_3} + a_4\alpha^{3i_4} = 0,\\
&a_1 + b + a_2 + a_3 + a_4 = 0,\\
&b = 0.
\end{aligned}$$

Since $b = 0$, the remaining equations are a special case of the equations for the previous partition. Hence $(a_1, a_2, a_3, a_4) = (0, 0, 0, 0)$.

Type (2,2,1). Suppose that

$$a_1\mathbf{A}_{i_1} + b_1\mathbf{B}_{i_1} + a_2\mathbf{A}_{i_2} + b_2\mathbf{B}_{i_2} + a_3\mathbf{A}_{i_3} = 0.$$

Then

$$\begin{aligned}
&a_1\alpha^{i_1} + b_1\alpha^{i_1} + a_2\alpha^{i_2} + b_2\alpha^{i_2} + a_3\alpha^{i_3} = 0,\\
&a_1\alpha^{3i_1} + b_1(\alpha^{3i_1} + \alpha^{i_1}) + a_2\alpha^{3i_2} + b_2(\alpha^{3i_2} + \alpha^{i_2}) + a_3\alpha^{3i_3} = 0,\\
&a_1 + b_1 + a_2 + b_2 + a_3 = 0,\\
&b_1 + b_2 = 0.
\end{aligned}$$

First we note that $b_2 = b_1 = b$, say. Hence $a_3 = a_1 + a_2$. The equations can be rewritten as follows:

$$(a_1 + b)\alpha^{i_1} + (a_2 + b)\alpha^{i_2} + (a_1 + a_2)\alpha^{i_3} = 0, \tag{24}$$

$$(a_1 + b)\alpha^{3i_1} + b(\alpha^{i_1} + \alpha^{i_2}) + (a_2 + b)\alpha^{3i_2} + (a_1 + a_2)\alpha^{3i_3} = 0. \tag{25}$$

Since $(a_1 + b) + (a_2 + b) + (a_1 + a_2) = 0$, at least one coefficient of (24) is 0. Hence the remaining two coefficients are also 0, that is

$$a_1 + b = a_2 + b = a_1 + a_2 = 0.$$

By (25) $b = 0$, and so $a_1 = a_2 = a_3 = 0$.

Type (3,1,1). Suppose that

$$a_1\mathbf{A}_{i_1} + b\mathbf{B}_{i_1} + c\mathbf{U} + a_2\mathbf{A}_{i_2} + a_3\mathbf{A}_{i_3} = 0.$$

Then

$$\begin{aligned}
&a_1\alpha^{i_1} + b\alpha^{i_1} + a_2\alpha^{i_2} + a_3\alpha^{i_3} = 0,\\
&a_1\alpha^{3i_1} + b(\alpha^{3i_1} + \alpha^{i_1}) + a_2\alpha^{3i_2} + a_3\alpha^{3i_3} = 0,\\
&a_1 + b + c + a_2 + a_3 = 0,\\
&b = 0.
\end{aligned}$$

Since $b = 0$, the first two equations imply that $a_1 = a_2 = a_3 = 0$ and so $c = 0$.

Type (3,2). Suppose that

$$a_1\mathbf{A}_{i_1} + b_1\mathbf{B}_{i_1} + c\mathbf{U} + a_2\mathbf{A}_{i_2} + b_2\mathbf{B}_{i_2} = 0.$$

Then

$$\begin{aligned}
&a_1\alpha^{i_1} + b_1\alpha^{i_1} + a_2\alpha^{i_2} + b_2\alpha^{i_2} = 0,\\
&a_1\alpha^{3i_1} + b_1(\alpha^{3i_1} + \alpha^{i_1}) + a_2\alpha^{3i_2} + b_2(\alpha^{3i_2} + \alpha^{i_2}) = 0,\\
&a_1 + b_1 + c + a_2 + b_2 = 0,\\
&b_1 + b_2 = 0.
\end{aligned}$$

First we note that $b_2 = b_1 = b$, say. The first two equations can be rewritten as follows:

$$(a_1 + b)\alpha^{i_1} + (a_2 + b)\alpha^{i_2} = 0, \tag{26}$$

$$(a_1 + b)\alpha^{3i_1} + b(\alpha^{i_1} + \alpha^{i_2}) + (a_2 + b)\alpha^{3i_2} = 0. \tag{27}$$

From (26) we get $a_1 + b = a_2 + b = 0$. From (27) we then get $b = 0$ and so $a_1 = a_2 = 0$. Hence $c = a_1 + a_2 + b_1 + b_2 = 0$.

Type (4,1). Suppose that

$$a_1\mathbf{A}_{i_1} + b\mathbf{B}_{i_1} + c\mathbf{U} + d\mathbf{V} + a_2\mathbf{A}_{i_2} = 0.$$

Then

$$\begin{aligned}
&a_1\alpha^{i_1} + b\alpha^{i_1} + a_2\alpha^{i_2} = 0,\\
&a_1\alpha^{3i_1} + b(\alpha^{3i_1} + \alpha^{i_1}) + a_2\alpha^{3i_2} = 0,\\
&a_1 + b + c + a_2 = 0,\\
&b + d = 0.
\end{aligned}$$

The first two equations can be rewritten as follows:

$$(a_1 + b)\alpha^{i_1} + a_2\alpha^{i_2} = 0, \tag{28}$$

$$(a_1 + b)\alpha^{3i_1} + b\alpha^{i_1} + a_2\alpha^{3i_2} = 0. \tag{29}$$

From (28) we get $a_1 + b = a_2 = 0$. Hence (29) implies that $b = 0$. Therefore $a_1 = 0$. Finally, $d = b = 0$ and $c = a_1 + a_2 + b = 0$.
Type (5). Suppose that

$$a\mathbf{A}_i + b\mathbf{B}_i + c\mathbf{U} + d\mathbf{V} + e\mathbf{A}_{i+1} = 0.$$

Then

$$\begin{aligned}
&a\alpha^i + b\alpha^i + e\alpha^{i+1} = 0,\\
&a\alpha^{3i} + b(\alpha^{3i} + \alpha^i) + e\alpha^{3(i+1)} = 0,\\
&a + b + c + e = 0,\\
&b + d = 0.
\end{aligned}$$

The first two equations can be rewritten as follows:

$$(a + b + e\alpha)\alpha^i = 0, \tag{30}$$

$$(a + b + e\alpha^3)\alpha^{3i} + b\alpha^i = 0. \tag{31}$$

From (30) we get $a + b = e = 0$. Hence (31) implies $b = 0$, and so $a = 0$. Finally, $d = b = 0$ and $c = a + b + e = 0$. $\square$

In particular, if α is a primitive element of $GF(2^m)$, then Theorem 4 gives an OOA$(5, 2m+2, 2^m-1)$ while the known construction in Section 2 applied to double-error-correcting BCH codes gives only OOA$(5, 2m+3, 2^m-1)$.

Note that the $[5n, 5n-2m-2]$ code which is the dual of the code D of Theorem 4 is a code in $H^{5,n}$ with minimum ordered distance 6.

6 Acknowledgement

Dr. Ferruh Özbudak got a copy of our manuscript some time ago. We thank him for useful comments and for pointing out some errors in the first table of Section 4. These have been corrected in the final revision. Dr. Ferruh Özbudak has also sent us a manuscript "A class of algebraic function field over finite fields with applications", where he developed a number of significant results inspired by the open problems of Section 4. For example, he has proved the existence of a primitive element $\alpha \in GF(2^m)$ satisfying (12) for all $m \geq 6$.

References

[1] R.C. Bose, Mathematical theory of the symmetrical factorial design, *Sankhya*, Vol. 8 (1947) pp. 128-139.

[2] Y. Edel and J. Bierbrauer, Construction of digital nets from BCH codes, In: Monte Carlo and Quasi-Monte Carlo Methods 1996 (Eds: H. Niederreiter et al.), Springer Lecture Notes in Statistics 127 (1998) pp. 221-231.

[3] G. Lachaud and J. Wolfmann, The weights of the orthogonals of the extended quadratic binary Goppa codes, *IEEE Trans. on Inform. Theory*, Vol. 36 (1990) pp. 686-692.

[4] K.M. Lawrence, A combinatorial interpretation of (t, m, s)-nets in base b, *Journal of Combinatorial Designs*, Vol. 4 (1996) pp. 275-293.

[5] K.M. Lawrence, A. Mahalanabis, G.L. Mullen and W.C. Schmid, Construction of digital (t, m, s)-nets from linear codes, In: Finite Fields and Applications (S.D. Cohen and H. Niederreiter, Eds.), Lect. Note series of the London Math. Soc., 233, Camb. Univ. Press, Cambridge (1996) pp. 189-208.

[6] V.I. Levenshtein, Split orthogonal arrays and maximum independent resilient systems of functions, *Designs, Codes and Cryptography*, Vol. 12, No. 2 (1997) pp. 131-160.

[7] W.J. Martin and D.R. Stinson, A generalized Rao bound for ordered orthogonal arrays and (t, m, s)-nets, *Canad. Math. Bull.*, Vol. 42, No. 3 (1999) pp. 359-370.

[8] W.J. Martin and D.R. Stinson, Association schemes for ordered orthogonal arrays and (t, m, s)-nets, *Canad. J. Math.*, Vol.51, No. 2 (1999) pp. 326-346.

[9] C. Moreno and O. Moreno, Exponential Sums and Goppa Codes: I, *Proc. Amer. Math. Soc.*, Vol. 111, No. 2 (1991) pp. 523-531.

[10] G.L. Mullen and W.C. Schmid, An equivalence between (t, m, s)-nets and strongly orthogonal hypercubes, *Journal of Combinatorial Theory, Ser. A*, Vol. 76 (1996) pp. 164-174.

[11] H. Niederreiter, Point sets and sequences with small discrepancy, *Monatsh. Math.*, Vol. 104 (1987) pp. 273-337.

[12] C.R. Rao, Factorial experiments derivable from combinatorial arrangements of arrays, *J. R. Stat. Soc.*, Vol. 89 (1947) pp. 128-139.

[13] M.Ju. Rozenblyum and M.A. Tsfasman, Codes for m-metric, *Problemy Peredachi Inform.*, Vol. 33, No. 1, 1977, 55-63 (in Russian). English translation *Problems of Inform. Trans.*, Vol. 33, No.1 (1977) pp. 45-52.

[14] I.M. Sobol', Distribution of points in a cube and the approximate evaluation of integrals, *Zh. Vychisl. Mat. i Mat. Fiz.*, Vol. 7, 1967, 784-802 (in Russian). English translation in *USSR Comput. Math. Math. Phys.*, Vol. 7 (1967) pp. 86-112.