Generalizing the Bierbrauer–Friedman bound for orthogonal arrays*

Denis S. Krotov, Ferruh Özbudak, Vladimir N. Potapov

We characterize mixed-level orthogonal arrays it terms of algebraic designs in a special multigraph. We prove a mixed-level analog of the Bierbrauer-Friedman (BF) bound for pure-level orthogonal arrays and show that arrays attaining it are radius-1 completely regular codes (equivalently, intriguing sets, equitable 2-partitions, perfect 2-colorings) in the corresponding multigraph. For the case when the numbers of levels are powers of the same prime number, we characterize, in terms of multispreads, additive mixed-level orthogonal arrays attaining the BF bound. For pure-level orthogonal arrays, we consider versions of the BF bound obtained by replacing the Hamming graph by its polynomial generalization and show that in some cases this gives a new bound.

Keywords: orthogonal array, algebraic t-design, completely regular code, equitable partition, intriguing set, Hamming graph, Bierbrauer–Friedman bound, additive codes.

1 Introduction

Orthogonal arrays are combinatorial structures important both for practical applications like design of experiments or software testing and theoretically, because

^{*}The work of D.K. was supported by the Natural Science Foundation of Hebei Province (project No. A2023205045) and within the framework of the state contract of the Sobolev Institute of Mathematics (FWNF2022-0017).

The work of F.Ö. was supported by TÜBİTAK under Grant 223N065.

[†]School of Mathematical Sciences, Hebei Key Laboratory of Computational Mathematics and Applications, Hebei Normal University, Shijiazhuang 050024, P. R. China;

Sobolev Institute of Mathematics, Novosibirsk 630090, Russia

[‡]Faculty of Engineering and Natural Science, Sabancı University, Istanbul, Turkey

[§]Faculty of Engineering and Natural Science, Sabancı University, Istanbul, Turkey

of many relations with coding theory, cryptography, design theory, etc., see e.g. [11]. Among many other interesting relations, pure-level, or symmetric, orthogonal arrays are known as a special case of algebraic designs, which makes them a part of a general theory that include also other widely known classes of combinatorial objects, such as combinatorial t-(v, k, λ) designs. One of the main results of this correspondence is establishing a similar relation for mixed-level (asymmetric) orthogonal arrays, attracting more attention last years, see e.g. recent works [4], [15], [16] and references there. Then, we use the correspondence obtained to generalize results known for pure-level orthogonal arrays, namely, the Bierbrauer–Friedman bound and constructions of arrays attaining it. Additionally, we consider some generalized versions of this bound for pure-level arrays that give a nontrivial inequality in cases when the original bound is not applicable.

The Bierbrauer–Friedman bound for pure-level orthogonal arrays with parameters OA(N, n, q, t) says that

$$N \ge q^n \left(1 - \left(1 - \frac{1}{q}\right) \frac{n}{t+1}\right),\tag{1}$$

see [9] for the case q=2 and [2] for general q. It is easy to see that the bound is nonnegative if and only if $t+1>\frac{q-1}{q}n$; so, it is effective for high values of t (in contrast, Rao's bound [17] is effective for relatively small t). The bound is tight, and there are orthogonal arrays constructed as linear [11, Section 4.3] or additive [1, Section 4.2] codes that attain it. Binary (q=2) orthogonal arrays attaining bound (1) whose size is not a power of 2 can be constructed as completely regular codes (see Definition 2 below) by the Fon-Der-Flaass construction [8]; the first example is OA(1536, 13, 2, 7). Ternary (q=3) arrays with the similar property were recently discovered, again in terms of completely regular codes, in [10]; the first example is OA($5 \cdot 3^8, 11, 3, 8$). For $q \geq 4$, the problem of existence of orthogonal arrays attaining bound (1) whose size is not a power of q or of its prime divisor remains open. Similar questions can be considered for mixed-level orthogonal arrays.

In this correspondence, we prove (Section 3) that (1) holds for mixed-level orthogonal arrays $OA(N, q_1 \cdot q_2 \cdot \ldots \cdot q_n, t)$ if we replace q^n by the product of all q_i s and $\frac{1}{q}$ by the average value of $\frac{1}{q_i}$. The arrays (we treat an array as a multiset of rows of length n) attaining this bound are necessarily simple sets (without repeated elements), independent sets (without pairs of elements at Hamming distance 1), and intriguing sets (completely regular codes with covering radius 1, see the definition below). The new bound is tighter than the previously known generalization [6]

$$N \ge q_{\rm m}^n \left(1 - \frac{n\tilde{q} - n}{n\tilde{q} + (t + 1 - n)q_{\rm M}}\right)$$
 if $n\tilde{q} + (t + 1 - n)q_{\rm M} > 0$, (2)

where $q_{\rm m}$, \tilde{q} , and $q_{\rm M}$ are respectively the minimum, the average, and the maximum value of q_i , $i=1,\ldots,n$. For example, for ${\rm OA}(N,2^14^4,3)$ the new bound is tight: $N\geq 64=2^9\cdot \left(1-\left(1-\frac{3}{10}\right)\frac{5}{3+1}\right)$ (see the construction in Example 1), while (2) gives $N\geq \frac{16}{7}=2^5\cdot \left(1-\frac{(3.6-1)\cdot 5}{4\cdot (3+1)-(4-3.6)\cdot 5}\right)$.

Further (Section 4), in the case when all q_i are powers of the same prime p, we prove that additive (linear over GF(p)) mixed-level orthogonal arrays attaining the Bierbrauer-Friedman bound are equivalent to special partitions of a vector space into subspaces, called multispreads [13].

Finally (Section 5), we discuss variations of bound (1) that can give positive values in the cases when the original bound (1) is negative. As an example, for $OA(N, n, 2, \frac{n}{2} - 1)$, n even, we obtain the bound

$$N > 0.409 \cdot n^{-1} \cdot 2^n.$$

To compare, for these parameters, Rao's bound gives the size of the Hamming ball of radius approximately n/4, which is $2^{h(\frac{1}{4})n(1+o(1))}$, $h(\frac{1}{4}) \simeq 0.8$.

Our main results are Theorem 7 (mixed orthogonal arrays are algebraic designs), Theorem 9 (Bierbrauer–Friedman bound for mixed-level orthogonal arrays and a relation with completely regular codes), Theorem 14 (the characterization of additive mixed-level orthogonal arrays attaining the Bierbrauer–Friedman bound), and Lemma 18 (a polynomial generalization of the Bierbrauer–Friedman bound for mixed-level orthogonal arrays).

2 Definitions and notations

By a graph, we will mean a multigraph, with multiple edges and loops allowed. A graph without loops and edge multiplicities more than 1 is called simple. For a graph G and a positive integer scalar s, sG denotes the graph on the same vertex set with all edge multiplicities multiplied by s. For two graphs G' = (V', E') and G'' = (V'', E''), $G' \square G''$ denotes their Cartesian product, the graph with the vertex set $V' \times V''$ and the edge (multi)set $\{\{(v_1, v), (v_2, v)\} : \{v_1, v_2\} \in E'$, $v \in V''\} \cup \{\{(v, v_1), (v, v_2)\} : \{v_1, v_2\} \in E''$, $v \in V''\}$.

For a positive integer s, the set $\{0, \ldots, s-1\}$ will be denoted by [s].

Definition 1 (adjacency matrix of a graph, eigenfunctions and eigenspaces). For a graph G = (V, E), the adjacency matrix A is the symmetric nonnegative integer $|V| \times |V|$ matrix whose rows and columns are indexed by V and the (x, y)th element $A_{x,y}$, $x, y \in V$, equals the multiplicity of $\{x, y\}$ in the edge multiset E. The eigenvectors of A, treated as functions from V to \mathbb{C} , are called eigenfunctions of G, or θ -eigenfunctions, where θ is the corresponding eigenvalue. An eigenspace of G is the subspace of the vector space \mathbb{C}^V consisting of the constantly zero

function and all θ -eigenfunctions for some eigenvalue θ . Since the adjacency matrix of a graph is symmetric, the eigenspaces are pairwise orthogonal.

Definition 2 (completely regular code with covering radius 1, $\{b; c\}$ -CR code). A set C of vertices of a regular graph G = (V, E) is called a *completely regular code* with covering radius 1 and intersection array $\{b; c\}$, where b, c > 0, or a $\{b; c\}$ -CR code, or simply a CR-1 code if for every vertex in V (in $V \setminus C$) the number of edges that connect it with $V \setminus C$ (respectively, with C), equals b (respectively, c).

Remark 1. In literature, CR-1 codes are studied under different names. They are also called *intriguing sets*; the corresponding partition of the vertex set into C and $V \setminus C$ is known as an equitable 2-partition or a 2-partition design; the corresponding 2-coloring of the vertex set is a perfect 2-coloring.

Definition 3 $(H(q_1 \cdot q_2 \cdot \ldots \cdot q_n))$, Hamming graph). For integers $q_1, q_2, \ldots, q_n \geq 2$, the graph $H(q_1 \cdot q_2 \cdot \ldots \cdot q_n)$ is the graph on the set of n-tuples from $V = [q_1] \times \ldots \times [q_n]$ with two n-tuples forming an edge of multiplicity μ if and only if they differ in only the ith position for some $i \in \{1, \ldots, n\}$ and $\mu = Q/q_i$, where $Q = \text{lcm}(q_1, \ldots, q_n)$ (least common multiple). If $q_1 = q_2 = \ldots = q_n = q$, then $H(q_1 \cdot q_2 \cdot \ldots \cdot q_n)$ is a simple graph known as a $Hamming\ graph$ and denoted H(n, q).

Definition 4 (algebraic t-design). For a regular graph G = (V, E) with eigenvalues $\theta_0 > \theta_1 > \ldots > \theta_d$ and the corresponding eigenspaces S_0, S_1, \ldots, S_d , a multiset C of its vertices is called an algebraic t-design (with respect to the natural descending ordering $\theta_0, \theta_1, \ldots, \theta_d$ of the graph eigenvalues) if in the decomposition

$$f_C = \varphi_0 + \varphi_1 + \ldots + \varphi_d, \qquad \varphi_i \in S_i,$$

of the multiplicity function f_C (in the case of a simple set, the characteristic function, indicator) of C we have $\varphi_1 = \ldots = \varphi_t \equiv 0$.

Definition 5 (orthogonal arrays, $OA(N, q_1 \cdot q_2 \cdot \ldots \cdot q_n, t)$). A nonempty multiset C of n-tuples from $V = [q_1] \times \ldots \times [q_n]$ is called an orthogonal array of strength t, $OA(|C|, q_1 \cdot q_2 \cdot \ldots \cdot q_n, t)$, if for any distinct i_1, \ldots, i_t from $\{1, \ldots, n\}$ and any $a_1 \in q_{i_1}, \ldots, a_t \in q_{i_t}$, the number of $(x_1, \ldots, x_n) \in C$ such that $x_{i_j} = a_j$, $j = 1, \ldots, t$, equals $\frac{|C|}{q_{i_1}q_{i_2} \cdots q_{i_t}}$ (i.e., independent on the choice of a_j , $j = 1, \ldots, t$). If $q_1 = q_2 = \ldots = q_n$, then such orthogonal arrays are called pure-level (in some literature, symmetric) and also denoted $OA(N, n, q_1, t)$; otherwise, they are called mixed-level, or just mixed (in some literature, asymmetric). For brevity, in the notation $q_1 \cdot q_2 \cdot \ldots \cdot q_n$, equal values of q_i can be grouped using degrees, e.g., $OA(N, 2 \cdot 2 \cdot 5, t)$ is the same as $OA(N, 2 \cdot 5, t)$, but not the same as $OA(N, 4 \cdot 5, t) = OA(N, 4 \cdot 5, t)$.

3 Orthogonal arrays and algebraic designs

We first describe the eigenspaces of the graph $H(q_1 \cdot q_2 \cdot ... \cdot q_n)$.

Lemma 6. The following functions form an orthogonal basis from eigenfunctions of $H(q_1 \cdot q_2 \cdot \ldots \cdot q_n)$:

$$\chi_{(b_1,b_2,\dots,b_n)}(x_1,x_2,\dots,x_n) = \xi_1^{b_1 x_1} \xi_2^{b_2 x_2} \dots \xi_s^{b_n x_n}, \qquad b_i \in [q_i], \tag{3}$$

where ξ_i is the degree- q_i primitive root of 1. Moreover, $\chi_{(b_1,b_2,...,b_n)}$ is an eigenfunction corresponding to the eigenvalue $\theta_w = k - wQ$, where

$$k = \sum_{i=1}^{n} \frac{Q}{q_i} (q_i - 1)$$

is the degree of $H(q_1 \cdot q_2 \cdot ... \cdot q_n)$, $Q = \text{lcm}(q_1, ..., q_n)$, and w is the number of nonzeros among $b_1, b_2, ..., b_n$.

Proof. The complete graph K_{q_i} has eigenfunctions $\xi_{(b_i)}(x_i) = \xi_i^{b_i x_i}$ corresponding to the eigenvalue $q_i - 1$ if $b_i = 0$ and -1 otherwise. After multiplying (the multiplicity of all edges of) K_{q_i} by $\frac{Q}{q_i}$, we get the same eigenfunctions with eigenvalues $\frac{Q}{q_i}(q_i - 1)$ and $-\frac{Q}{q_i}(q_i - 1)$. We note that the difference Q between these two eigenvalues does not depend on i.

The rest is straightforward from the following easy property of the Cartesian product of graphs, see e.g. [3, Section 1.4.6]: if $\chi'(x')$, $x' \in V'$, and $\chi''(x'')$, $x'' \in V''$, are θ' - and θ'' -eigenfunctions of graphs $\Gamma' = (V', E')$ and $\Gamma'' = (V'', E'')$, respectively, then $\chi(x', x'') = \chi'(x')\chi''(x'')$ is a $(\theta' + \theta'')$ -eigenfunction of $\Gamma' \Box \Gamma''$.

The following fact generalizes Delsarte's characterization [5, Theorem 4.4] of pure-level orthogonal arrays as algebraic designs.

Theorem 7. A multiset C of words from $V = [q_1] \times ... \times [q_n]$ is an orthogonal array $OA(|C|, q_1 \cdot q_2 \cdot ... \cdot q_n, t)$ if and only if C is an algebraic t-design in $H(q_1 \cdot q_2 \cdot ... \cdot q_n)$.

Proof. If. Assume C is an algebraic t-design and f_C is its multiplicity function. We need to show that the sum of f_C over $V^{a_1,\dots,a_t}_{i_1,\dots,i_t}$ does not depend on the choice of a_1,\dots,a_t , where $1 \leq i_1 < \dots < i_t \leq n, \ a_j \in [q_{i_j}], \ \text{and} \ V^{a_1,\dots,a_t}_{i_1,\dots,i_t}$ denotes the set of all n-tuples (x_1,\dots,x_n) from V such that $x_{i_1}=a_1,\dots,x_{i_t}=a_t$.

We have

$$f_C = \varphi_0 + \varphi_{t+1} + \varphi_{t+2} + \ldots + \varphi_n,$$

where φ_i is the zero constant or a θ_i -eigenfunction of $H(q_1 \cdot q_2 \cdot ... \cdot q_n)$.

For $i \geq t+1$, each such eigenfunction is a linear combination of basis eigenfunctions $\chi_{(b_1,\ldots,b_n)}$ from (3), where the number of nonzero elements among b_1 , ..., b_n is i. We claim that

(*) for more than t nonzeros in (b_1, \ldots, b_n) , the sum of $\chi_{(b_1, \ldots, b_n)}$ over $V_{i_1, \ldots, i_t}^{a_1, \ldots, a_t}$ equals 0. Indeed, denoting by l_1, \ldots, l_s the indices from $\{1, \ldots, n\} \setminus \{i_1, \ldots, i_t\}$, s = n - t, we have

$$\sum_{(x_1,\dots,x_n)\in V_{i_1,\dots,i_t}^{a_1,\dots,a_t}} \chi_{(b_1,\dots,b_n)}(x_1,\dots,x_n)$$

$$= \xi_{i_1}^{b_{i_1}a_{i_1}} \cdot \dots \cdot \xi_{i_t}^{b_{i_t}a_{i_t}} \cdot \sum_{x_{l_s}=0}^{q_{l_1}} \xi_{l_1}^{b_{l_1}x_{l_1}} \cdot \dots \cdot \sum_{x_{l_s}=0}^{q_{l_s}} \xi_{l_s}^{b_{l_s}x_{l_s}}. \quad (4)$$

Since the number of nonzeros is larger than t, for at least one j from $\{l_1, \ldots, l_s\}$ we have $b_j \neq 0$. It follows that at least one sum in (4) equals 0, which proves (*).

From (*) we conclude that the sum of f_C over $V_{i_1,\ldots,i_t}^{a_1,\ldots,a_t}$ equals the sum of ϕ_0 over $V_{i_1,\ldots,i_t}^{a_1,\ldots,a_t}$. Since ϕ_0 is a constant, the sum does not depend on the choice of a_1,\ldots,a_t .

Only if. We need to show that f_C is orthogonal to the θ_i -eigenspace for every i in $\{1,\ldots,t\}$, i.e., to all $\chi_{(b_1,\ldots,b_n)}$ with more than 0 and at most t nonzeros in (b_1,\ldots,b_n) . Let all i such that $b_i\neq 0$ lie in $\{i_1,\ldots,i_t\}$, where $1\leq i_1<\ldots< i_t\leq n$. For the standard scalar product $(f_C,\chi_{(b_1,\ldots,b_n)})$ of f_C and $\chi_{(b_1,\ldots,b_n)}$, we have

$$(f_{C}, \chi_{(b_{1}, \dots, b_{n})}) = \sum_{(x_{1}, \dots, x_{n}) \in V} \chi_{(b_{1}, \dots, b_{n})}(x_{1}, \dots, x_{n}) \cdot f_{C}(x_{1}, \dots, x_{n})$$

$$\stackrel{(i)}{=} \sum_{(x_{1}, \dots, x_{n}) \in V} \xi_{i_{1}}^{b_{i_{1}} x_{i_{1}}} \cdot \dots \cdot \xi_{i_{t}}^{b_{i_{t}} x_{i_{t}}} \cdot f_{C}(x_{1}, \dots, x_{n})$$

$$= \sum_{a_{1}=0}^{q_{i_{1}}-1} \dots \sum_{a_{t}=0}^{q_{i_{t}}-1} \sum_{(x_{1}, \dots, x_{n}) \in V_{i_{1}, \dots, i_{t}}^{a_{1}, \dots, a_{t}}} \xi_{i_{1}}^{b_{i_{1}} x_{i_{1}}} \cdot \dots \cdot \xi_{i_{t}}^{b_{i_{t}} x_{i_{t}}} \cdot f_{C}(x_{1}, \dots, x_{n})$$

$$= \sum_{a_{1}=0}^{q_{i_{1}}-1} \xi_{i_{1}}^{b_{i_{1}} a_{1}} \cdot \dots \cdot \sum_{a_{t}=0}^{q_{i_{t}}-1} \xi_{i_{t}}^{b_{i_{t}} a_{t}} \cdot \sum_{(x_{1}, \dots, x_{n}) \in V_{i_{1}, \dots, i_{t}}^{a_{1}, \dots, a_{t}}} f_{C}(x_{1}, \dots, x_{n})$$

$$\stackrel{(ii)}{=} \sum_{a_{1}=0}^{q_{i_{1}}-1} \xi_{i_{1}}^{b_{i_{1}} a_{1}} \cdot \dots \cdot \sum_{a_{t}=0}^{q_{i_{t}}-1} \xi_{i_{t}}^{b_{i_{t}} a_{t}} \cdot |C|/q_{i_{1}} \dots q_{i_{t}} \stackrel{(iii)}{=} 0,$$

where in equality (i) we use that $\xi_j^{b_j x_j} = 1$ if $b_j = 0$, in (ii) we use the definition of an orthogonal array, and (iii) holds because for some j in $\{i_1, ..., i_t\}$ we have $b_j \neq 0$ and hence $\sum_{a=0}^{q_j} \xi_j^{b_j a} = 0$. We have shown that f_C is orthogonal to $\chi_{(b_0, ..., b_n)}$ for any $(b_0, ..., b_n)$ with more than 0 and less than t+1 nonzeros. Hence, C is an algebraic t-design.

Now, we can apply the following lower bound on the size of an algebraic design in a regular graph.

Lemma 8 ([14, Sect. 4.3.1]). The cardinality of an algebraic t-design C in a k-regular graph G = (V, E) with eigenvalues $k = \theta_0 > \theta_1 > \ldots > \theta_d$ satisfies the inequality

 $\frac{|C|}{|V|} \ge \frac{-\theta_{t+1}}{k - \theta_{t+1}}.\tag{5}$

Moreover, a multiset C of vertices of G is an algebraic t-design meeting (5) with equality if and only if C is a simple set (without multiplicities more than 1) and a $\{k; -\theta_{t+1}\}$ -CR code.

The following bound was proved in [9] for $q_1 = \ldots = q_s = 2$ and in [2] for $q_1 = \ldots = q_s = q$ for any q. The theorem generalizes the mentioned results to the case of mixed-level orthogonal arrays.

Theorem 9. For an orthogonal array C with parameters $OA(N, q_1 \cdot ... \cdot q_n, t)$, we have

$$N \ge q_1 q_2 ... q_n \left(1 - \left(1 - \frac{1}{q} \right) \frac{n}{t+1} \right), \tag{6}$$

where q is the harmonic mean of all q_i , i.e., $\frac{1}{q} = \frac{1}{n} \sum_{i=1}^{n} \frac{1}{q_i}$.

Moreover, a multiset of vertices of the graph $H = H(q_1 \cdot ... \cdot q_n)$ is an $OA(|C|, q_1 \cdot ... \cdot q_n, t)$ meeting (6) with equality if and only if C is a simple set (without multiplicities more than 1) and a $\{k; -\theta_{t+1}\}$ -CR code, where $k = Qn(1 - \frac{1}{q})$ (the degree of H) and $\theta_{t+1} = k - (t+1)Q$, $Q = \text{lcm}(q_1, \ldots, q_n)$.

Proof. Taking into account Theorem 7 and Lemma 8, it remains to check that (5) and (6) are the same for G = H. Indeed, the degree of H is

$$k = \frac{Q}{q_1}(q_1 - 1) + \dots + \frac{Q}{q_n}(q_n - 1) = Qn - Q\left(\frac{1}{q_1} + \dots + \frac{1}{q_n}\right) = Qn\left(1 - \frac{1}{q}\right)$$

and $\theta_i = k - iQ$. So, we find

$$\frac{-\theta_{t+1}}{k - \theta_{t+1}} = \frac{(t+1)Q - k}{(t+1)Q} = 1 - \left(1 - \frac{1}{q}\right)\frac{n}{t+1}.$$

Next, we compare the new bound with the previous generalization (2) of (1) to mixed-level orthogonal arrays [6].

Proposition 10. For mixed-level orthogonal arrays, bound (6) is tighter than (2).

Proof. Rewriting (2) in a convenient form, we have to prove that

$$q_1 q_2 ... q_n \left(1 - \left(1 - \frac{1}{q}\right) \frac{n}{t+1}\right) \ge q_m^n \left(1 - \left(1 - \frac{1}{\tilde{q}}\right) \frac{1}{1 - \left(1 - \frac{t+1}{n}\right) \frac{q_M}{\tilde{q}}}\right),$$

where

$$q_{\rm m} \le q \le \tilde{q} \le q_{\rm M},\tag{7}$$

$$1 - \frac{t+1}{n} \ge 0,\tag{8}$$

$$1 - \left(1 - \frac{t+1}{n}\right) \frac{q_{\mathcal{M}}}{\tilde{q}} \ge 0 \tag{9}$$

((7) are known inequalities between the minimum, the harmonic mean, the arithmetic mean, and the maximum values; (8) is from t < n for nontrivial orthogonal arrays; (9) means that the denominator in (2) is positive, which is the condition of the applicability of (2)). The required inequality is straightforward from the following three observations.

- (i) Trivially, $q_1q_2...q_n \ge q_m^n$.
- (ii) From (7) we have $1 \frac{1}{q} \le 1 \frac{1}{\tilde{q}}$.
- (iii) Taking into account (7)–(9), we get

$$\frac{n}{t+1} = \frac{1}{1 - (1 - \frac{t+1}{n})} \le \frac{1}{1 - (1 - \frac{t+1}{n})\frac{q_{\mathbf{M}}}{\tilde{q}}}.$$

Finally, each of (i), (ii), (iii) turns to equality if and only if $q_1 = q_2 = \ldots = q_n$, i.e., for pure-level arrays.

Remark 2. As noted in [6], the definition of an orthogonal array implies that N must be a multiple of

$$S = LCM \{q_{i_1}q_{i_2} \dots q_{i_t} : 0 < i_1 < \dots < i_t\}.$$

In particular, this gives the bound $N \geq S$ (by similarity of arguments, it can be considered as an analog of the Singleton bound for error-correcting codes), but also means that any bound of form $N \geq B(q_1 \cdot \ldots \cdot q_n, t)$ can be rounded to

$$N \ge \lceil B(q_1 \cdot \ldots \cdot q_n, t) / S \rceil \cdot S. \tag{10}$$

However, in some cases bound (6) is already divisible by S, and the problem of existence orthogonal arrays attaining it arises. In the next section, we show how to construct such arrays in the case when all q_i are powers of the same prime number.

4 Additive mixed orthogonal arrays attaining the Bierbrauer–Friedman bound

In this section, all q_i are powers of the same prime p, and $[p^i]$ is associated with the vector space \mathbb{F}_p^i (to be explicit, an integer a in $[p^i]$ can be associated with its p-based notation, treated as a vector from \mathbb{F}_p^i). We should warn the reader about the following difference in notation: now q_i denotes p^i , not the number of levels (alphabet size) in the ith position. This is because in this section, it is convenient to write parameters in the form $OA(N, q_1^{n_1}q_2^{n_2} \dots q_s^{n_s}, t)$ (all q_i are different, but some n_i , i < s, can be zero), while in Section 3 the preferred form was $OA(N, q_1 \cdot q_2 \cdot \ldots \cdot q_n, t)$, where q_i are not necessarily distinct.

Definition 11 (additive code). A set of $(n_1 + \ldots + n_s)$ -tuples from $V = (\mathbb{F}_p^1)^{n_1} \times (\mathbb{F}_p^2)^{n_2} \times \ldots \times (\mathbb{F}_p^s)^{n_s}$, where p is prime, is called *additive* (an additive code, or an additive orthogonal array if we consider it as an orthogonal array) if it is closed with respect to the coordinatewise addition, i.e., forms a subspace of the $(n_1 + 2n_2 + \ldots + sn_s)$ -dimensional vectorspace V over \mathbb{F}_p .

Remark 3. For prime p, "additive" and " \mathbb{F}_p -linear" are the same, but in general, if p is a prime power, \mathbb{F}_p -linear codes form a proper subclass of additive codes. The theory in the rest of this section keeps working for an arbitrary prime power p if we replace "additive" by " \mathbb{F}_p -linear" everywhere. However, to simplify reading, we focus on the most important case of prime p and localize the arguments for the general case in this remark.

Any k-dimensional vector subspace C of an n-dimensional vector space S_n can be represented as the null-space (kernel) of a homomorphism from S to an (n-k)-dimensional vector space S_{n-k} over the same field. If the bases in S_n and S_{n-k} , are fixed, such a homomorphism is represented by an $(n-k) \times n$ matrix, called a check matrix of C. In our case the dimension of the space is $(n_1+2n_2+\ldots+sn_s)$, we have a natural basis, and the coordinates of a vector, as well as the columns of a check matrix, are naturally divided into $n_1 + n_2 + \ldots + n_s$ groups, blocks, the first n_1 blocks of size 1, the next n_2 blocks of size 2, and so on. For a check matrix H, by $H_{i,j}$ we denote the space spanned by the columns from the jth block of size i.

Definition 12 (multifold partition of a space). A multiset D of subspaces of a vector space S is called a μ -fold partition of S if every nonzero vector of S belongs to exactly μ subspaces from D, respecting the multiplicities.

Next, we define two concepts, which are not (in contrast to Definition 12) key concepts in our theory, but allow to mention additionally one important correspondence in the main theorem of this section.

Definition 13 (one-weight code, alphabet-effective code). An additive code C in V is called *one-weight* (of weight w) if the number of nonzero blocks in a nonzero codeword is constant (equal to w). The code is called *alphabet-effective* if in each block, every element of the corresponding alphabet \mathbb{F}_p^i occurs in some codeword (so, the alphabet \mathbb{F}_p^i is effectively used).

Theorem 14. Let H be an $m \times (n_1 + 2n_2 + \ldots + sn_s)$ rank-m matrix over \mathbb{F}_p , and let C be the null-space of H (so, C is an additive code in $(\mathbb{F}_p^1)^{n_1} \times \ldots \times (\mathbb{F}_p^s)^{n_s}$). Denote

$$k = \sum_{i=1}^{s} n_i (p^s - p^{s-i}) = p^s \sum_{i=1}^{s} n_i (1 - p^{-i}), \quad \mu = \frac{k}{p^m - 1}, \quad q_i = p^i.$$
 (11)

The following assertions are equivalent:

- (i) C is an $OA(|C|, q_1^{n_1}q_2^{n_2}...q_s^{n_s}, t)$ attaining bound (6);
- (i') C is an $OA(|C|, q_1^{n_1}q_2^{n_2}...q_s^{n_s}, t)$ with $t = \frac{\mu + k}{p^s} 1$;
- (ii) C is a $\{k, \mu\}$ -CR code in $H(q_1^{n_1}q_2^{n_2}...q_s^{n_s})$;
- (iii) the code C^{\perp} generated by the rows of H is an alphabet-effective one-weight code of weight p^{m-s} ;
- (iv) the multiset $M = \{p^{s-i} \times H_{i,j}\}_{i=1}^{s} \text{ of subspaces of } \mathbb{F}_p^m \text{ is a } \mu\text{-fold partition } (p^{s-i} \times H_{i,j} \text{ denotes that } H_{i,j} \text{ is added } p^{s-i} \text{ times in the multiset});$
- (v) the collection $M^{\perp} = \{H_{i,j}^{\perp}\}_{i=1}^{s}$ of subspaces dual to $H_{i,j}$ is a ν -fold partition of \mathbb{F}_p^m , where $\nu = n_1 + \ldots + n_s p^{m-s} \cdot \mu$.

Proof. Since C is a null-space of H, we have $|C| = p^{n_1+2n_2+...+sn_s}/p^m = q_1^{n_1} \cdot q_2^{n_2} \cdot ... \cdot q_s^{n_s}/p^m$.

(i) \iff (i') Taking into account the expression for |C| above, (6) has the form

$$p^{-m} \ge \left(1 - \left(1 - \frac{1}{q}\right) \frac{n}{t+1}\right). \tag{12}$$

(recall that q is the harmonic mean of $\underbrace{q_1,...,q_1}_{n_1 \text{ times}},\underbrace{q_2,...,q_2}_{n_2 \text{ times}},...,\underbrace{q_s,...,q_s}_{n_s \text{ times}}$). From the equality in (12), we find

$$t+1 = \frac{n(1-\frac{1}{q})}{1-p^{-m}} = \frac{p^{-s}k}{1-p^{-m}} = p^{-s}k(1+\frac{1}{p^m-1}) = \frac{k+\mu}{p^s}.$$

Inversely, substituting $t = \frac{k+\mu}{p^s} - 1$ turns (12) to equality.

- (i) \iff (ii) By Theorem 9, C attains (6) if and only if it is a $\{k; -\theta_{t+1}\}$ -CR code, where k is the degree of $H(q_1^{n_1}q_2^{n_2}...q_s^{n_s})$ and $\theta_{t+1} = k p^s(t+1)$ (the (t+1)th largest eigenvalue of $H(q_1^{n_1}q_2^{n_2}...q_s^{n_s})$, counting from 0).
- (ii) ⇐⇒(iv) Assume that (iv) holds and we have to show (ii). We first check that
 - (*) $H_{i,j}$ has dimension i for each i, j.

Indeed, if it is so, then $H_{i,j}$ has (p^i-1) nonzero points, $p^{s-i} \times H_{i,j}$ has (p^s-p^{s-i}) nonzero points, and M has $\sum_{i=1}^s n_i(p^s-p^{s-i})$, i.e., k, nonzero points. This is exactly the number of points we need to cover all p^m-1 nonzero points of \mathbb{F}_p^m with multiplicity $\mu = \frac{k}{p^m-1}$.

But if one $H_{i,j}$ has dimension smaller than i, then the number of points in M is not enough to make a μ -fold partition of \mathbb{F}_p^m . So, (*) holds.

Next, (*) means that C is independent. Indeed, if there are two adjacent vectors x and y in C, then their difference x - y has nonzero values only in coordinates from one block, say (i, j)th. In this case, these values are coefficients of a nontrivial linear dependency between the corresponding columns, and hence $H_{i,j}$ has dimension smaller than i, contradicting (*).

The independence of C implies that every its element is connected to elements not in C by k edges (k is the degree of the graph), and it remains to confirm the second parameter μ of the $\{k; \mu\}$ -CR code.

For a vector v not in C denote by s its $syndrome\ H \cdot v^{\mathrm{T}}$ (since $c \notin C$, the syndrome s is nonzero). A vector v - e is adjacent to v and belongs to C if and only if $H \cdot e^{\mathrm{T}} = s$ and e has zeros in all positions out of one block, say (i, j)th. The last is equivalent to $s \in H_{i,j}$. Since the subspace $H_{i,j}$ is counted with multiplicity p^{s-i} in the multiset M, and the multiplicity of the edge $\{v, v - e\}$ is also p^{s-i} , the number of edges between v and C is equal to the multiplicity of s in M, i.e., μ .

By reversing the arguments, we ensure that (ii) implies (iv).

- (iv) \iff (v) The equivalence between (iv) and (v) is proven in [13, Theorem 3] (which is, apart of the direct correspondence between the parameters, is essentially a special case of [7, Theorem 15]).
- (iv) \iff (iii) The equivalence between (iv) and (iii) is essentially proven in [13, Theorem 1]. The difference is that [13, Theorem 1] considers one-weight codes over the same alphabet \mathbb{F}_p^s (in our current notation), but not necessarily alphabet-effective. It remains to observe that there is a trivial weight-preserving relation between alphabet-effective additive codes over our mixed alphabet and additive codes over the alphabet \mathbb{F}_p^s , namely, adding s-i zero columns to each block of size $m \times i$ of the generator matrix H.

A collection of subspaces of \mathbb{F}_p^m of dimension at most s satisfying the condition of Theorem 14 is called a $(\lambda, \mu)_p^{s,m}$ -multispread [13], where $\lambda = n_1(p^{s-1} - 1) + n_2(p^{s-1} - 1)$

 $n_2(p^{s-2}-1)+\ldots+n_{s-1}(p^1-1)$ (the multiplicity of the zero vector in M). Theorem 14 means that such multispreads with n_i subspaces of dimension i, $i=1,\ldots,s$, corresponds to orthogonal arrays in $(\mathbb{F}_p^1)^{n_1}\times\ldots\times(\mathbb{F}_p^s)^{n_s}$ attaining the generalized Bierbrauer-Friedman bound (6) in Theorem 9. Note that n_1,\ldots,n_s are not uniquely determined from the parameters p,s,m,λ,μ of a $(\lambda,\mu)_p^{s,m}$ -multispread, and even without fixing n_1,\ldots,n_s the problem of existence of $(\lambda,\mu)_p^{s,m}$ -multispread is open in general (in [13], it is completely solved for s=2, any p, and for $p^s \in \{2^3, 2^4, 3^3\}$). The pure-level subcase of Theorem 14 was proved in [1, Theorem 4.8]; in that case, $\lambda=0$, and multispreads are μ -fold spreads, whose parameters are characterized, see [12, p.83], [7, Corollary 8].

Example 1. Consider the $3 \times (1 \cdot 1 + 4 \cdot 2)$ matrix

$$H = \left(\begin{array}{cccccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right)$$

over \mathbb{F}_2 . Its null-space is an additive $OA(64, 2^14^4, 3)$. Indeed, $64 = 2^9 (1 - (1 - \frac{3}{10}) \frac{5}{3+1})$; the degree of the graph $H(2^14^4) = 2K_2 \times K_4 \times K_4 \times K_4 \times K_4$ is $1+4\cdot 3 = 14$; the eigenvalue $\theta_{t+1} = \theta_4$ equals $14 - 4 \cdot 4 = -2$; the subspace $H_{1,1} = \langle (1,1,1) \rangle$, corresponding to the first column, is taken with multiplicity 2 and covers the vector (1,1,1) exactly $2 = -\theta_4$ times; each of the other nonzero vectors from \mathbb{F}_2^3 is covered exactly $2 = -\theta_4$ times by the subspaces $H_{2,1} = \langle (1,0,0), (0,1,0) \rangle$, $H_{2,2} = \langle (1,0,0), (0,0,1) \rangle$, $H_{2,3} = \langle (0,1,0), (0,0,1) \rangle$, $H_{2,4} = \langle (1,1,0), (0,1,1) \rangle$, formed by the last four blocks of columns. So, $\mu = 2$ According to p.(iv) of Theorem 14, the dual subspaces $H_{1,1}^{\perp}$, $H_{2,1}^{\perp}$, $H_{2,2}^{\perp}$, $H_{2,3}^{\perp}$, $H_{2,4}^{\perp}$ form a partition of \mathbb{F}_2^3 , $\nu = n_1 + n_2 - \mu \cdot 2^{m-s} = 1 + 4 - 2 \cdot 2^{3-2} = 1$.

5 Polynomial generalization of the Bierbrauer–Friedman bound

For a connected graph G, d(G) denotes its diameter, and $G^{(j)}$, denotes a simple graph where two vertices are adjacent if and only if the distance between them in G is j.

Definition 15 (distance-regular graph). A simple connected graph is called a distance-regular graph if for i = 1, ..., d(G) the product $A^{(1)}A^{(i)}$ is a linear combination of $A^{(i-1)}$, $A^{(i)}$, and $A^{(i+1)}$, where $A^{(j)}$ is the adjacency matrix of $G^{(j)}$.

Corollary 16. For every distance-regular graph G, there are degree-i polynomials $K^{(i)}$, i = 0, ..., d(G), such that $G^{(i)} = K^{(i)}(G)$.

Let G be a distance-regular graph. Consider a nonnegative integer linear combination of the polynomials $K^{(i)}$, i.e., $P = \sum_i \alpha_i K^{(i)}$, $a_i \geq 0$. Then P(A) is the adjacency matrix of a multigraph P(G) with the same set V of vertices. If vertices u and v are at distance i from each other in G, then the edge $\{u, v\}$ has multiplicity α_i in P(G). The proposition below collects some obvious and straightforward facts.

Proposition 17. (a) The set of eigenfunctions of P(G) includes the set of eigenfunctions of G. If P is strictly monotonic function, then these sets coincide.

- (b) If φ is an eigenfunction of G with eigenvalue θ , then φ is also an eigenfunction of P(G) with eigenvalue $P(\theta)$.
- (c) If P strictly increases, then the sets of algebraic t-designs of G and P(G) coincide.

The next lemma is a variant of Lemma 8.

Lemma 18. Let G = (V, E) be a distance-regular graph with eigenvalues $k = \theta_0, \theta_1, \dots, \theta_{d(G)}$, in the decreasing order, let the polynomial P be a linear combination

$$P(x) = \alpha_1 K^{(1)}(x) + \ldots + \alpha_{d(G)} K^{(d(G))}(x)$$

of the polynomials $K^{(1)}$ from Corollary 16, where $\alpha_i \geq 0$, i = 1, ..., d(G), and let

$$\mu = \max \{ P(\theta_{t+1}), \dots, P(\theta_{d(G)}) \}.$$

If $\mu < 0$, then the cardinality of an algebraic t-design C satisfies the inequality

$$\frac{|C|}{|V|} \ge \frac{-\mu}{P(k) - \mu}.\tag{13}$$

Proof. If all α_i are integer, then P(x) is a graph, for which Lemma 8 gives (13). If all α_i are rational, we divide P by their greatest common divisor, which makes all α_i integer and does not affect the value in (13).

If some α_i are irrational, we can approximate them by rational values with any accuracy and get (13) as the limit of bounds corresponding to polynomials P with rational coefficients.

Our aim is to find a polynomial P such that $\theta_{t+1} \geq 0$ but $\mu < 0$. In this case, the lower bound from Lemma 8 is non-positive and hence trivial, while the lower bound from Lemma 18 is positive and can be valuable. Actually, to obtain the best lower bound in (13), we need to solve the following linear programming problem in the variables $\alpha_1, \ldots, \alpha_{d(G)}, \mu$ (the last one is an additional variable,

which plays the role of $\max\{P(\theta_j)\}_{j\geq t+1}$:

$$\begin{cases} \sum_{i=1}^{\operatorname{d}(G)} \alpha_i K^{(i)}(\theta_j) \leq \mu, & j = t+1, \dots, \operatorname{d}(G), \\ \alpha_i \geq 0, & i = 1, \dots, \operatorname{d}(G), \end{cases}$$

$$\begin{cases} \operatorname{d}(G) \\ \sum_{i=1}^{\operatorname{d}(G)} a_i K^{(i)}(\theta_0) = \operatorname{const} & (\text{the degree of } P(G)), \\ \mu \longrightarrow \min. \end{cases}$$

By the proof of Lemma 18, we do not need to care about the integrity of α_i . By Lemmas 8, 18, and Proposition 17(c) we can conclude the following.

Proposition 19. Let a collection $a_1, \ldots, a_{d(G)}$ be the solution of the linear program and let P be the corresponding polynomial. Suppose that $P(\theta_{t+1}) \neq P(\theta_j)$ for $j \neq t+1$. If some t-design C attains the bound (13), then C is a CR-1 code in G.

For the Hamming graph G = H(n,q), the degree-w polynomial $K^{(w)}$ is

$$K^{(w)}(\cdot) = P_w(P_1^{-1}(\cdot)),$$
where $P_w(x) = P_w(x; n, q) = \sum_{j=0}^w (-1)^j (q-1)^{w-j} \binom{x}{j} \binom{n-x}{w-j}$

is the Krawtchouk polynomial; $P_1(x) = (q-1)n - qx$, $P_1^{-1}(y) = \frac{(q-1)-y}{q}$.

Example 2. Consider G = H(2m, 2), t = m - 1. Let us derive a bound on the size of AO(N, 2m, 2, m - 1) by combining only three polynomials $K^{(i)}$, i = 1, 2, 3. We have G = H(2m, 2), $\theta_{t+1} = \theta_m = 0$,

$$K^{(1)}(x) = x$$
, $K^{(2)}(x) = \frac{1}{2}(x^2 - 2m)$, $K^{(3)}(x) = \frac{1}{6}(x^3 - (6m - 2)x)$.

We are looking for a polynomial $P=K^{(3)}+\beta K^{(2)}+\alpha K^{(1)}$ where $\alpha\geq 0,\ \beta\geq 0,$ and $P'(x)\geq 0$ for all $x\in [-2m,0]$. Put $\alpha=\frac{\beta^2}{2}+m-\frac{1}{3}$. Then $6P(x)=(x+\beta)^3-\beta^3-6\beta m$. It is easy to see that P increases monotonically. Substituting $\beta=\frac{m}{\sqrt{3}},$ we obtain $6P(x)=x^3+\sqrt{3}mx^2+m^2x-2\sqrt{3}m^2$ and, by (13),

$$\frac{|C|}{|V|} \ge \frac{-6P(0)}{6P(2m) - 6P(0)} = \frac{2\sqrt{3}m^2}{10m^3 + 4\sqrt{3}m^3} = \frac{1}{m(5 \cdot 3^{-\frac{1}{2}} + 2)} > \frac{0.2046}{m}.$$

6 Conclusion

The most general contribution of our correspondence is a representation of orthogonal arrays as algebraic designs (which was previously known only for pure-level arrays). More specifically, as an application of this representation, we have considered two possibilities to generalize the Bierbrauer–Friedman bound for orthogonal arrays.

One of the generalizations concerns mixed-level orthogonal arrays, and we have also show how to construct arrays attaining the generalized bound. However, the constructed arrays have one restriction because of their additive structure over a finite field; namely, the size of such an array is always a prime power. As was mentioned in the introduction, the only known arrays attaining the Bierbrauer–Friedman bound with the size not being a prime power are pure-level binary or ternary. With generalizing the bound the problem of the existence of such arrays also expands to the mixed-level case. In particular: do there exist mixed-level $OA(N, 2^{n_1}3^{n_2}, t)$ attaining bound (6)? Orthogonal arrays attaining the considered bound (in both pure- and mixed-level cases) are of special interest because of their relation with such regular structures as CR-1 codes (equivalently, intriguing sets, equitable 2-partitions, perfect 2-colorings).

The other, polynomial, generalization, considered in Section 5, makes it possible to obtain a lower bound on the size of a pure-level orthogonal array in the cases when the original Bierbrauer–Friedman bound gives a trivial inequality. The authors do not know if it is possible to improve the Bierbrauer–Friedman bound in this way in cases when it is positive.

References

- [1] E. A. Bespalov, D. S. Krotov, A. A. Matiushev, A. A. Taranenko, and K. V. Vorob'ev. Perfect 2-colorings of Hamming graphs. *J. Comb. Des.*, 29(6):367–396, June 2021. https://doi.org/10.1002/jcd.21771.
- [2] J. Bierbrauer. Bounds on orthogonal arrays and resilient functions. J. Comb. Des., 3(3):179-183, 1995. https://doi.org/10.1002/jcd.3180030304.
- [3] A. E. Brouwer and W. H. Haemers. *Spectra of Graphs*. Springer-Verlag, New York, 2012. https://doi.org/10.1007/978-1-4614-1939-6.
- [4] Guangzhou Chen and Xiaodong Niu. Constructions for new orthogonal arrays based on large sets of orthogonal arrays. *Des. Codes Cryptography*, 91(7):2605–2625, 2023. https://doi.org/10.1007/s10623-023-01217-5.

- [5] P. Delsarte. An Algebraic Approach to Association Schemes of Coding Theory, volume 10 of Philips Res. Rep., Supplement. N.V. Philips' Gloeilampenfabrieken, Eindhoven, 1973.
- [6] W. S. Diestelkamp. Parameter inequalities for orthogonal arrays with mixed levels. *Des. Codes Cryptography*, 33(3):187–197, 2004. https://doi.org/10.1023/B:DESI.0000036245.92856.fo.
- [7] S. El-Zanati, G. Seelinger, P. Sissokho, L. Spence, and C. Vanden Eynden. On λ -fold partitions of finite vector spaces and duality. *Discrete Math.*, 311(4):307–318, 2011. https://doi.org/10.1016/j.disc.2010.10.026.
- [8] D. G. Fon-Der-Flaass. Perfect 2-colorings of a hypercube. Sib. Math. J., 48(4):740-745, 2007. https://doi.org/10.1007/s11202-007-0075-4 translated from Sib. Mat. Zh. 48(4) (2007), 923-930.
- [9] J. Friedman. On the bit extraction problem. In Foundations of Computer Science, IEEE Annual Symposium on, pages 314–319, Los Alamitos, CA, USA, 1992. IEEE Computer Society. https://doi.org/10.1109/SFCS.1992.267760.
- [10] S. Goryainov and D. Krotov. Completely regular codes in graphs covered by a Hamming graph. arXiv eprint 2411.09698, DOI10.48550/arXiv.2411.09698, 2024.
- [11] A. S. Hedayat, N. J. A. Sloane, and J. Stufken. *Orthogonal Arrays. Theory and Applications*. Springer Series in Statistics. Springer, New York, NY, 1999. https://doi.org/10.1007/978-1-4612-1478-6.
- [12] J. W. P. Hirschfeld. *Projective Geometries Over Finite Fields*. Oxford University Press, New York, 1979.
- [13] D. S. Krotov and I. Yu. Mogilnykh. Multispreads. E-print 2312.07883, arXiv.org, 2023. Available at http://arxiv.org/abs/2312.07883.
- [14] D. S. Krotov and V. N. Potapov. Completely regular codes and equitable partitions. In M. Shi and P. Solé, editors, *Completely Regular Codes in Distance Regular Graphs*, chapter 1. CRC Press, 2024. To appear.
- [15] X. Lin, S. Pang, and J. Wang. Construction of asymmetric orthogonal arrays with high strength. Stat, 13(4):e70011(1–12), Dec. 2024. https://doi.org/10.1002/sta4.70011.
- [16] X. Niu, G. Chen, Q. Gao, and S. Pang. New results on asymmetric orthogonal arrays with strength $T \ge 3$. jDM, 348(2):114264(1-14), Feb. 2025. https://doi.org/10.1016/j.disc.2024.114264.

[17] C. R. Rao. Factorial experiments derivable from combinatorial arrangements of arrays. J. R. Stat. Soc., Suppl., 9(1):128–139, 1947. https://doi.org/10.2307/2983576.