Sofia University "St. Kliment Ohridski"
Faculty of Mathematics and Informatics

Tedis Ramaj

Algebraic methods for studying some combinatorial configurations and their applications

PhD Thesis
for awarding the Ph.D. degree
in the Professional field 4.5 Mathematics

Doctor program "Algebra, topology and applications"

Supervisors:

Associate prof. PhD Silvia Boumova

Associate prof. PhD Maya Stoyanova

Contents

Introduction

In 1940 Rao introduced certain combinatorial arrangements named orthogonal arrays. They play important roles in statistics (used in designing experiments), computer science and cryptography. Orthogonal arrays are related to combinatorics, finite fields, geometry and error-correcting codes. Although much has been done in this area, there are still many unsolved problems. [17]

Definition 0.0.1. *(**Definition 1.1.1**) Let $\mathcal{A}$ be an alphabet of q symbols. An **Orthogonal Array** $OA(M, n, q, t)$ **of strength** t **with** M **rows,** n **columns** $(n \geq t)$**, and** q **levels** is an $M \times n$ matrix (array) with entries from $\mathcal{A}$ so that every $M \times t$ submatrix contains each of the q^t possible t-tuples equally often as a row (say λ times).*

Obviously $M = \lambda q^t$ and an orthogonal array of strength t is also of strength t', for any $t' < t$. The number λ is called ***index*** of the orthogonal array.

Often used notations for $OA(M, n, q, t)$ are also $OA(M, q^n, t)$ or $t - (q, n, \lambda)$.

Here is an example of $OA(4, 3, 2, 2)$:

$$\begin{matrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{matrix}$$

The origin of orthogonal arrays is experimental statistic. C. R. Rao ([30, 31, 32]) introduced them for use in fractional factorial experiments. Since their introduction many researchers coming from different scientific arrays began to contribute to the subject. The diversity of their background has caused various terms to be used for one and the same notions in the area. Here are the most used terms for the basic parameters of $OA(M, n, q, t)$:

$\mathcal{A}^n$**:** full factorial design;

$OA(M, n, q, t)$**:** fractional factorial design; fraction;

M**:** number of rows, or number of experimental runs, or size;

n**:** number of columns, or number of factors, or number of constraints; number of variables;

q**:** number of levels; number of symbols;

t**:** strength, or estimability of parameters;

λ**:** index;

Generally $OA(M, n, q, t)$ is a multi-subset of $\mathcal{A}^n$, that is, it can have repeated rows, but all its different rows form a subset of $\mathcal{A}^n$. Orthogonal array without repeated rows is called ***simple***.

For instance $t-(q, t, \lambda)$, that is, $OA(\lambda q^t, t, q, t)$ is a trivial example of an orthogonal array: each element of $\mathcal{A}^t$ is repeated λ times.

Usually $\mathcal{A} = \mathbb{Z}_q$, the additive group of integers modulo q, or the finite field $GF(q)$, when q is a prime power. The use of the finite field $GF(q)$ as alphabet enables results from coding theory to be drawn in for solving problems concerning orthogonal arrays. But there are researchers which consider orthogonal arrays over $\mathbb{C}_q$, the multiplicative group of q-roots of unity in $\mathbb{C}$ ($\mathbb{Z}_q \cong \mathbb{C}_q$) or other specific alphabets.

The notion orthogonal array can be generalized to so called ***mixed orthogonal array***. Let $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n$ be a set of alphabets with cardinality $q_1, q_2, \ldots, q_n$, respectively. A mixed orthogonal array is defined as a multi-subset of $\mathcal{A}_1 \times \mathcal{A}_2 \times \cdots \times \mathcal{A}_n$ satisfying the properties given in Definition 1.1.1.

Some applications of orthogonal arrays in medicine are in:

- **pharmaceutical companies**. Based on orthogonal arrays, they conduct studies on stability and shelf life of drugs, which involves many different factors.
- **multiple drug therapy**. Orthogonal arrays can help doctors to adjust dose levels to avoid or minimize interactions when using multiple medications.
- **clinical trials** to study how drugs are absorbed, distributed, metabolized, and restricted by the body, especially to study the effects of multiple factors on these drug characteristics.

In experiments the joint effect of several factors on the properties of a product or process is studied. And usually they are conducted according to an orthogonal array. The terminology used is as follows: each column corresponds to a factor n, the symbols are the factor levels q and each row represents a combination of the factor levels, called runs.

The number of rows M (which represents the number of runs in the experiment and may require too many resources) should be reduced. This brings us to the following problems:

1. to find the smallest possible number of rows of orthogonal array;

2. for a given number of runs to know the largest number of columns that can be used in an orthogonal array.

Or more generally these are problems of

⋆ **Existence:** for which values of the number of rows, columns, strength and levels does an orthogonal arrayexist?

⋆ **Construction:** how can we construct an array, if one exists.

⋆ **Non-isomorphic classes:** find the numbers of non-isomorphic orthogonal arrays for given parameters.

In what follows we continue with a more detailed description of the results in chapters. Definitions, concepts and theorems are introduced to describe the results obtained in the Phd dissertation. The corresponding numbers are also given.

In Chapter 1 we give some notations and properties of Orthogonal arrays.

Proposition 0.0.2. *(**Proposition 1.2.1, [17]**) For an $OA(M, n, q, t)$ the following properties hold*

(i) Remind that the parameters of an orthogonal array satisfy the equality $\lambda = \frac{M}{q^t}$

(ii) A permutation of the symbols (levels q) of any factor (column n) in an $OA(M, n, q, t)$ results in orthogonal array with the same parameters.

(iii) A permutation of the runs or factors (columns n) in an $OA(M, n, q, t)$ results in orthogonal array with the same parameters.

(iv) Any $M \times k$ sub-array of $OA(M, n, q, t)$ is an $OA(M, k, q, t')$, where $t' = \min\{t, k\}$.

(v) If $A = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}$ *is an* $OA(M, n, q, t)$*, where* A_1 *itself is an* $OA(M_1, n, q, t_1)$*, then* A_2 *is an* $OA(M - M_1,\ n,\ q,\ t_2)$ *with* $t_2 \geq \min\{t, t_1\}$.

The definitions for codes and its relations to orthogonal arrays are given in section 1.3.

Special attention is paid to Krawtchouk's polynomials which are introduced in 1929 by Ukrainian mathematician Krawtchouk as a generalization of Hermite polynomials. They play an important role in coding theory and are also useful in graph theory and number theory (see, e.g., [22, 15], [19], [41], and [25]). .

Let Euclidean space E be a linear space over the field of real numbers $\mathbb{R}$ supplied with usual scalar product.

Let $E \subset \mathbb{R}[x]$ be the linear space of polynomials of degree up to n. The bilinear map defined by

$$\langle f, g\rangle \stackrel{def}{=} \sum_{i=0}^{n} k_i f(x_i) g(x_i), \quad k_i \geq 0,$$

where $(x_0, x_1, \ldots, x_n) \in \mathbb{R}^{n+1}$ is a fixed $(n+1)$-tuple of different real numbers called ***approximation points***, satisfies the axioms for scalar product. Usually the ***weight vector*** $(k_0, k_1, \ldots, k_n)$ is chosen to satisfy $\sum_{i=0}^{n} k_i = 1$ in order to assure that the norm is 1.

Let $q \geq 2$ be integer, $(0, 1, \ldots, n)$ be the approximation points, and

$$\langle f, g\rangle \stackrel{def}{=} \frac{1}{q^n} \sum_{i=0}^{n} \binom{n}{i} (q-1)^i f(i) g(i). \tag{1}$$

The weight vector is

$$\frac{1}{q^n}\left(1,\ \binom{n}{1}(q-1),\ \ldots,\ \binom{n}{n}(q-1)^n\right)$$

and satisfies

$$\sum_{i=0}^{n} \binom{n}{i} \frac{(q-1)^i}{q^n} = 1.$$

Definition 0.0.3. ***(Definition 1.4.1) Krawtchouk polynomial*** *is a polynomial defined by*

$$K_k(x;\, n, q) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j} (q-1)^{k-j}, \quad k = 0, 1 \ldots n.$$

Usually n and q have already been fixed or their values are known from context.

Hence for simplicity we often omit n and q and write only $K_k(x)$.

The Krawtchouk polynomial $K_k(x;\, n, q)$ is a polynomial of degree k in x with leading coefficient $(-q)^k/k!$. Here are the first three polynomials:

$$\begin{aligned}
&K_0(x) = 1;\\
&K_1(x) = -qx + n(q-1);\\
&K_2(x) = \frac{1}{2}\Big[q^2x^2 - \big((2n-1)(q-1)+1\big)x + n(n-1)(q-1)^2\Big].
\end{aligned}$$

The generating function of Krawtchouk polynomials is

$$\sum_{k=0}^{n} K_k(x;\, n, q)z^k = \Big(1 + (q-1)z\Big)^{n-x}(1-z)^x. \tag{2}$$

Proposition 0.0.4. *(**Proposition 1.4.2**) Krawtchouk polynomials satisfy the relations*

$$(q-1)^i\binom{n}{i}K_k(i) = (q-1)^k\binom{n}{k}K_i(k). \tag{3}$$

Lemma 0.0.5. *(**Lemma 1.4.3**) Krawtchouk polynomials $K_0(x), K_1(x), \ldots, K_n(x)$ form an orthogonal system regarding to the scalar product (1, 1.1), namely*

$$\langle K_k, K_l\rangle = \frac{1}{q^n}\sum_{i=0}^{n}\binom{n}{i}(q-1)^i K_k(i)K_l(i) = \binom{n}{k}(q-1)^k\,\delta_{kl} \tag{4}$$

for $k, l = 0, 1, \ldots, n$, where δ_{kl} is Kronecker delta.

The second orthogonality relation is as follows.

Corollary 0.0.6. *(**Corollary 1.5**)*

$$\sum_{i=0}^{n} K_k(i)K_i(l) = q^n\delta_{kl} \tag{5}$$

Theorem 0.0.7. *(**Theorem 1.4.5**) For any polynomial $f(x) \in \mathbb{R}[x]$ of degree $\le n$ there is a unique expansion*

$$f(x) = \sum_{k=0}^{n} f_k K_k(x), \qquad \textit{where}$$

$$f_k = \frac{1}{q^n\binom{n}{k}(q-1)^k}\sum_{i=0}^{n}\binom{n}{i}(q-1)^i f(i)K_k(i) = \frac{1}{q^n}\sum_{i=0}^{n} f(i)K_i(k).$$

The orthogonal polynomials have many interesting properties (see [41]). The following theorem gives some of them.

Theorem 0.0.8. *(**Theorem 1.4.10**) The following relations hold:*

(i) $K_k(x;\, n) = (q-1)K_{k-1}(x;\, n-1) + K_k(x;\, n-1)$;

(ii) $(q-1)K_k(x;\, n) + K_k(x-1;\, n) = qK_k(x-1;\, n-1)$;

(iii) $\sum_{k=0}^{n} \binom{n-k}{n-j} K_k(x) = q^j \binom{n-x}{j}$;

(iv) $\sum_{k=0}^{m} K_k(x;n) = K_m(x-1;n-1)$.

Using the attractive and beautiful properties of additive characters (Section 1.4.4) we can prove the theorems that can help a lot in our investigations in the field of orthogonal arrays.

Definition 0.0.9. *(**Definition 1.5.1**) Let C be an $OA(M,n,q,t)$ (or a subset of $\mathcal{A}^n$) and $\mathbf{x} \in \mathcal{A}^n$ be a fixed vector. The set of integers $\mathbf{p}(\mathbf{x}) = (p_0, p_1, \ldots, p_n)$ defined by*

$$p_i = |\{\mathbf{u} \in C \mid d(\mathbf{x},\mathbf{u}) = i\}|$$

*is called the **distance distribution of C with respect to $\mathbf{x}$**.*

The lemma below is due to Delsart ([14, 13])

Lemma 0.0.10. *(**Lemma 1.5.2, Delsart[14, 13]**) Let C be $OA(M,n,q,t)$ and $\mathbf{x} \in \mathcal{A}^n(\mathbb{F}_q^n)$. If $\mathbf{p}(\mathbf{x}) = (p_0, p_1, \ldots, p_n)$ is the distance distribution of C with respect to $\mathbf{x}$ then*

$$\sum_{i=0}^{n} p_i K_k(i) = 0 \qquad \text{for } k = 1, \ldots, t. \tag{6}$$

Theorem 0.0.11. *(**Theorem 1.5.3**) Let C be $OA(M,n,q,t)$ and $\mathbf{v} \in \mathbb{F}_q^n$. If $\mathbf{p}(\mathbf{v}) = (p_0, p_1, \ldots, p_n)$ is the distance distribution of C with respect to $\mathbf{v}$ then for any polynomial $f(x)$ of degree $\deg f \le t$ the following hold*

(a)

$$\sum_{i=0}^{n} p_i f(i) = f_0 M, \qquad f_0 = \frac{1}{q^n}\sum_{i=0}^{n} f(i)K_i(0) = \frac{1}{q^n}\sum_{i=0}^{n} \binom{n}{i}(q-1)^i f(i) \tag{7}$$

where $f(x) = f_0 + \sum_{j=1}^{t} f_j K_j(x)$.

(b)

$$\sum_{i=0}^{n} p_i f(t_i) = a_0 M, \qquad a_0 = \frac{1}{q^n}\sum_{i=0}^{n}\binom{n}{i}(q-1)^i f(t_i) = \frac{1}{q^n}\sum_{i=0}^{n} K_i(0) f(t_i) \quad (8)$$

where $f(x) = a_0 + \sum_{j=1}^{t} a_j Q_j(x)$ *and* $t_i = 1 - \frac{2i}{n}$.

In chapter 2 are used polynomial and combinatorial techniques [13, 23, 17] to compute all feasible distance distributions of ternary orthogonal arrays of respectively small lengths and strengths. We propose a method for computing and reducing of the possibilities of distance distributions of given orthogonal arrays. We use properties of orthogonal arrays (with given parameters) and some relations with their derived orthogonal arrays to reduce the possible distance distributions. To solve questions about existence and classification, it is important to know the possible distance distributions of an orthogonal array with respect to any point. Having this information we can get knowledge about its structure.

We improve the know methods [7, 8, 2] for computing and reducing the possibilities for distance distributions of orthogonal arrays. Then apply the new conditions so that the orthogonal arrays are satisfied. If no then we get nonexistence result, i.e there is no $OA(108, 16, 3, 3)$ and confirm the nonexistence result for $OA(108, 17, 3, 3)$ ([2]).

Let C be an $OA(M, n, q, t)$ and $\mathbf{x} \in \mathcal{A}^n$ be a fixed vector. The set of integers $\mathbf{p}(\mathbf{x}) = (p_0, p_1, \ldots, p_n)$ defined by

$$p_i = |\{\mathbf{u} \in C \mid \mathrm{d}(\mathbf{x}, \mathbf{u}) = i\}|$$

is called the **distance distribution of C with respect to $\mathbf{x}$**.

Boyvalenkov and co-authors ([7, 8, 3]) point out that in the general case all feasible distance distributions can be computed as nonnegative integer solutions of certain system of linear equations with Vandermone matrix (t_j^i), where $t_j = 1 - \frac{2j}{n}, j = 0, \ldots, n$.

Recently, the results of Bose and Bush ([1]) were proved by Manev ([26]) in a different way. The Manev's results are summarized in the Theorem 2.1.2. This theorem can facilitate the fast computation of the distance distributions.

Theorem 0.0.12 (Theorem 2.1.2, [26]). *Let C be an $OA(M, n, q, t)$ and $\mathbf{v} \in \mathcal{A}^n$. If $\mathbf{p}(\mathbf{v}) = (p_0, p_1, \ldots, p_n)$ is the distance distribution of C with respect to $\mathbf{v}$, then for $m = 0, 1, \ldots, t$ and $s = 1, \ldots, t+1$, $\mathbf{p}(\mathbf{v})$ satisfies the following systems:*

(i)

$$\sum_{i=0}^{n}\binom{n-i}{m}p_i=\frac{M}{q^m}\binom{n}{m}=\lambda q^{t-m}\binom{n}{m};$$

(ii)

$$\sum_{i=0}^{n}p_i i^m=\frac{M}{q^n}\sum_{i=0}^{n}\binom{n}{i}i^m(q-1)^i;$$

(iii)

$$\sum_{i=0}^{n}p_i(n-i)^m=\frac{M}{q^n}\sum_{i=0}^{n}\binom{n}{i}(n-i)^m(q-1)^i;$$

(iv)

$$\sum_{i=0}^{n}\binom{i-s}{m}p_i=\frac{M}{q^n}\sum_{i=0}^{n}\binom{n}{i}\binom{i-s}{m}(q-1)^i.$$

These systems (2.2, 2.3, 2.4, 2.5) show that $(p_0, p_1, ..., p_n)$ is a solution of equavalent linear systems with nonnegative integer coefficients. One should find all their nonnegative integer solutions, that is, to select the nonnegative among all integer solutions.

In the section 2.2 we present an algorithm for determining possible vectors $\mathbf{p}$. It turns out that finding the best possible upper bound vector u for the vectors p is very important. This increases the efficiency of the computations.

Beginning with considering the system (iv) in Theorem 2.1.2 in details.

$$A_s p^\tau = a, \tag{9}$$

where

$$A_s=(a_{kl})=\left(\binom{l-s}{k}\right)$$

is a $(t+1)\times(n+1)$ matrix. The vector $a=(a_0,a_1,\ldots,a_t)^\tau$ is determined by

$$a_k=\frac{M}{q^n}\sum_{i=0}^{n}\binom{n}{i}\binom{i-s}{k}(q-1)^i,$$

where $k=0,\ldots,t$. Columns of A corresponding to $l=s,\ldots,s+t$ form $(t+1)\times(t+1)$ matrix $R_t=(r_{ij})=(\binom{j}{i})$. Multiplying the system (9, 3.1) with R_t^{-1} we get $Bp^\tau=b$, where $B=R_t^{-1}A=(b_{ml})$ and $b=(b_0,\ldots,b_t)^\tau$, that is,

$$b_{ml}=(-1)^m\sum_{j=0}^{t}(-1)^j\binom{j}{m}\binom{l-s}{j},\quad m=0,1,\ldots,t,\ l=0,1,\ldots,n$$

and

$$b_m = (-1)^m \lambda q^{t-n} \sum_{i=0}^{n} \left(\binom{n}{i} (q-1)^i \sum_{j=0}^{t} \binom{j}{m} \binom{i-s}{j} \right), \quad m = 0, 1, \ldots, t.$$

The analytic expressions of the transformed matrix that we received in the following theorem helps a lot in computations.

Theorem 0.0.13. *(**Theorem 2.3.1**) The following hold:*

(a) $b_{ml} = (-1)^{2m} \binom{l-s}{m} \binom{t-l+s}{t-m} = \binom{l-s}{m} \binom{t-l+s}{t-m}$;

(b) $$b_{ml} = \begin{cases} (-1)^{m+t} \dfrac{l-s-t}{l-s-m} \binom{t}{m} \binom{l-s}{t}, & l \neq s+m \\ 1, & l = s+m \end{cases}$$

It turns out that there is no good simple form of expression for b_m in general, only in special cases. After simplification (described in detail in Chapter 2 - applying Lemma 2.1.6 to (2.8) we obtain

$$b_m = (-1)^m \lambda q^{t-n} \sum_{i=0}^{n} \binom{n}{i} (q-1)^i (-1)^m \binom{i-s}{m} \binom{t+s-i}{t-m}$$

or equivalently

$$b_m = (-1)^{m+t} \lambda q^{t-n} \binom{t}{m} \sum_{i=0}^{n} \binom{n}{i} \binom{i-s}{t} \frac{i-s-t}{i-s-m} (q-1)^i,$$

where $m = 0, 1, \ldots, t$.

Some bounds could be found when strength t is even number. The situation when t is odd number is a more complicate.

Corollary 0.0.14. ***(Corollary 2.3.3)*** *For t even number the inequality holds*

$$p_l \leq \left\lfloor \frac{b_m}{b_{ml}} \right\rfloor, \text{ for } l = 0, 1, ..s-1, s+t+1, \ldots, n$$

In section 2.4. we study orthogonal arrays applying the knowledge of possible distance distributions and derive information about its structure.

Let C be an $OA(M, n, q, t)$ and we can assume that C contains the all-zero vector. Let C' be the orthogonal array obtained from C by deleting the first column. Denote by $C_i,\ i = 0, 1, \ldots, q-1$ the set obtained by taking all rows of C with the i-th element

of $\mathcal{A}$ in the first column and then deleting the first column. (C_0 corresponds to 0 in the first column.) According to Proposition 1.2.1

$$C' \text{ is } OA(M, n-1, q, t) \qquad \text{and} \qquad C_i \text{ is } OA(M/q, n-1, q, t-1).$$

We compute all possible distance distributions of C', C_i, C using described algorithm, and any other necessary arrays derived from C.

Let $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in C$, i.e., $\mathbf{c}_0 = (c_2, \ldots, c_n) \in C_0$ or C_i. The distance distribution of C with respect to $\mathbf{c}$ is $\mathbf{p}(\mathbf{c}) = (p_0, p_1, \ldots, p_n)$ and $\mathbf{p}^0(\mathbf{c}_0) = (p_0^0, p_1^0, \ldots, p_{n-1}^0)$ of C_0 (or C_i) to $\mathbf{c}_0$, respectively.

A vector $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ ***dominate*** another vector $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ if $a_i \geq b_i$ for all $i = 1, \ldots, n$.

Corollary 0.0.15. *(**Corollary 2.4.1**) If vector $p = (p_0, p_1, \ldots, p_n)$ is a a distance distribution of $OA(M, n, q, t)$ array C then it satisfies the following conditions*

(i) $(p_0, p_1, \ldots, p_{n-1})$ *dominates* $(p_0^0, p_1^0, \ldots, p_{n-1}^0)$, *when* $p_0^0 \geq 1$;

(ii) $(p_1, p_2, \ldots, p_n)$ *dominates* $(p_0^0, p_1^0, \ldots, p_{n-1}^0)$ *when* $p_0^0 = 0$;

(iii) *the difference*

$$\overline{p}(c_0) = (\bar{p}_0, \bar{p}_1, \ldots, \bar{p}_{n-1}) = (p_1 - p_1^0, \ldots, p_{n-1} - p_{n-1}^0, p_n)$$

has to be the distance distribution of $C_1 \cup \cdots \cup C_{q-1}$ with respect to the external point c_0;

(iv) $\overset{\mathrm{v}}{p}(c_0) = \overline{p}(c_0) + p^0(c_0)$ *has to be a distance distribution of* $\overset{\mathrm{v}}{C}$ *with respect to* c_0.

Deleting different columns we can obtain not only different C_i but different values for $\mathbf{p}$, $\overline{\mathbf{p}}(\mathbf{c})$, $\mathbf{p}^0$. The following result holds

Theorem 0.0.16. *(**Theorem 2.4.2 [[7, 26]]**) Let $\overline{p}^{(1)}, \overline{p}^{(2)}, \ldots, \overline{p}^{(s)}$ be all possible successors of p and let $\overline{p}^{(i)}$ be obtained in k_i cases of deleting of a column, $i = 1, 2, \ldots, s$. Then the integers k_i satisfy*

$$\begin{cases} k_1 + k_2 + \cdots + k_s = n \\ k_1\overline{p}^{(1)} + k_2\overline{p}^{(2)} + \cdots + k_s\overline{p}^{(s)} = (p_1, 2p_2, \ldots, np_n) \\ k_i \geq 0 \end{cases}$$

In section 2.5. we prove that

Theorem 0.0.17. *(**Theorem 2.5.1**) The minimal index for ternary arrays with strength $t = 3$ and length 17 and 16 is $\lambda = 5$.*

Some structural results are shown in section 2.5.1.

Remark: All the computations are made in Maple.

In Chapter 3 we consider another connection between codes and orthogonal arrays, i.e. **covering radius** ([5]). The covering radius of an orthogonal array C is the minimum of the numbers ρ such that every point of the Hamming space $H(n, q)$ is within distance ρ of at least one point in C; that is, it is the smallest radius such that closed balls of that radius centered at the points of C have all of $H(n, q)$ as their union.

We obtain analytically upper bounds for the covering radius of a given orthogonal array depend on its parameters. We have done this by investigations of the set of all feasible distance distributions of the corresponding orthogonal array and related to it orthogonal arrays.

To prove our bounds for covering radius we choose to work with $s = n - t$. This makes the situation simpler, i.e.

$$Bp^{\tau} = b, \text{ and } B = (UI_{t+1}) = (b_{ml}),$$

where $b = (b_m),\ m = 0, 1, \ldots, t,\ l = 0, 1, \ldots, n.$

The coefficients b_0 and b_1 can be expressed.

Corollary 0.0.18. *(**Corollary 3.2.1**) For given parameters M, n, q, t, $s = n - t$, and $\lambda = M/q^t$ the following hold:*

(i) $b_0 = \lambda\binom{n}{t}$;

(ii) $b_1 = -\lambda\binom{n}{t-1}(n - t - q + 1)$.

The next theorem gives the first bounds on covering radius for a given orthogonal array.

Theorem 0.0.19. *(**Theorem 3.2.2**) Let C be an $OA(M, n, q, t)$ having covering radius $\rho(C)$. Then*

$$\rho(C) \leq n - t.$$

The uniqueness of the solution in the proof of Theorem 3.2.2 allows further improvements.

Distance distributions with maximum number of zeros in the beginning	$\rho(C)$	Theorem 3.2.2,3.2.3
$OA(54, 5, 3, 3)$ $(0, 0, 20, 0, 30, 4)$ **Sloane's page** [40]	2	$\rho(C)$ $\leq 5 - 3 = 2$ $n - t = q - 1$
$OA(18, 7, 3, 2)$ $(0, 0, 0, 0, 14, 0, 0, 4)$ **Evangelaras, Koukouvinos, Lappas** [16] **Schoen, Eendebak, Nguyen**[34]	4	$\rho(C)$ $\leq 7 - 2 - 1 = 4$ $n - t > q - 1$

Table 1: Examples of covering radius of orthogonal arrays that attain the bounds from Theorems 3.2.2, 3.2.3

Theorem 0.0.20. *(**Theorem 3.2.3**) Let C be an $OA(M, n, q, t)$ having covering radius $\rho(C)$. If $n - t > q - 1$, then*

$$\rho(C) \leq n - t - 1.$$

Using a procedure for reduction of the possible distance distributions of orthogonal array we improve the bound by 1 under certain assumptions.

Theorem 0.0.21. *(**Theorem 3.3.1**) Let C be an $OA(M, n, q, t)$ with covering radius $\rho(C)$. If $n > 2(t + q - 1)$, then*

$$\rho(C) \leq n - t - 2.$$

Some examples that attain the bounds are pointed out.

Acknowledgement

I would like to express my gratitude to my supervisors associate prof. PhD Silvia Boumova and associate prof. PhD Maya Stoyanova for their valuable advices, guidance and help.

I would like to thank all colleagues from the Algebra section of FMI, Sofia University for the pleasant and stimulating atmosphere during the preparation of the

Sloane's page [40], Distance distributions with maximum number of zeros in the beginning	$\rho(C)$	Theorem 3.3.1
$OA(27, 13, 3, 2)$ $[0, 0, 0, 0, 0, 0, 0, 13, 0, 0, 13, 0, 0, 1]$	7	$\rho(C)$ $\leq 13 - 2 - 2 = 9$
$OA(36, 13, 3, 2)$ $[0, 0, 0, 0, 0, 0, 0, 10, 14, 0, 6, 4, 0, 2]$	7	$\rho(C)$ $\leq 13 - 2 - 2 = 9$
$OA(729, 14, 3, 4)$ $[0, 0, 0, 0, 0, 14, 42, 42, 133, 126,$ $210, 70, 84, 0, 8]$	5	$\rho(C)$ $\leq 14 - 4 - 2 = 8$

Table 2: Examples of covering radius of orthogonal arrays

dissertation.

Author's contribution

According to the author, the main contributions of the Ph.D thesis are the following

1. We develop a combinatorial method for computing and reducing the possibilities of distance distributions of ternary orthogonal array of given parameters $OA(M, n, q, t)$.

2. We receive analytical expression of the matrix (Theorem 2.3.1) used for evaluating the distance distributions of a given orthogonal array. This helps a lot in faster calculation of distance distributions.

3. The main result is nonexistence of $OA(108, 17, 3, 3)$ and $(108, 16, 3, 3)$ ternary orthogonal arrays. The result of nonexistence of $OA(108, 17, 3, 3)$ was already obtained by M. Stoyanova and T. Marinova, but we receive it independently using another approach. We wrote a paper together [2].

4. We obtain analytically upper bounds for the covering radius of orthogonal arrays.

5. We apply a procedure for reduction of the possible distance distributions of orthogonal array to improve the bound by one under certain assumptions.

Publications

The results described in the dissertation are published in the following papers.

1. ([6]) **S. Boumova, T. Ramaj, M. Stoyanova**, *Computing distance distributions of ternary orthogonal arrays. Comptes rendus de l'Académie bulgare des Sciences, 2020, ISSN (print):1310–1331 , ISSN (online):2367–5535, to appear.* (*SJR (Scopus):0.218, JCR-IF (Web of Science):0.343*).

2. ([2]) **S. Boumova, T. Marinova, T. Ramaj, M. Stoyanova**, Nonexistence of (17, 108, 3) ternary orthogonal array, *Annual of Sofia University "St. Kliment Ohridski", Faculty of Mathematics and Informatics, vol:106, 2019, pages:117-126, ISSN (print):1313-9215, ISSN (online):2603-5529, Ref, MathSciNet.*

3. ([5]) **S. Boumova, T. Ramaj, M. Stoyanova**, On Covering Radius of Orthogonal Arrays, *Proceedings of Seventeenth International Workshop on Algebraic and Combinatorial Coding Theory ACCT 2020, October 11-17, 2020, Bulgaria* (accsepted in IEEE Xplore),

All papers are co-authored with S. Boumova and M. Stoyanova. One of them is co-authored by S. Boumova, M. Stoyanova and T. Marinova.

The results have been presented at international and national conferences and forums as follows

Conference talks

1. ([5]) **S. Boumova, T. Ramaj, M. Stoyanova**, On Covering Radius of Orthogonal Arrays, *Proceedings of Seventeenth International Workshop on Algebraic and Combinatorial Coding Theory, October 11-17, 2020, Bulgaria (online).*

2. **S. Boumova, P. Boyvalenkov, T. Ramaj, M. Stoyanova**, Some bounds for Covering Radius of Orthogonal Arrays, *Annual Workshop on Coding Theory "Prof. Stefan Dodunekov", October 8-11, 2020, Bulgaria (online).*

3. ([4]) **S. Boumova, P. Boyvalenkov, T. Ramaj, M. Stoyanova**, Computing distance distributions of ternary orthogonal arrays, *The 14th Annual Meeting of the Bulgarian Section of SIAM, 2019, December 17-19, Bulgaria.*

4. **S. Boumova, T. Ramaj, M. Stoyanova**, Distance distributions of ternary orthogonal arrays, *Spring Science Session FMI, 2019.*

5. **S. Boumova, T. Ramaj, M. Stoyanova**, Computing distance distributions of ternary orthogonal arrays, *Annual Workshop on Coding Theory "Prof. Stefan Dodunekov", November 21-24, 2019, Troyan, Bulgaria.*

6. **S. Boumova, T. Ramaj, M. Stoyanova**, Orthogonal Arrays and Related Objects I, *Annual Workshop on Coding Theory "Prof. Stefan Dodunekov", November 8-11, 2018, Veliko Turnovo, Bulgaria.*

Declaration of originality of results

I hereby declare that this dissertation contains original results obtained by me with the support and assistance of my supervisors. The results obtained by other scientists are described in detail and cited in the bibliography.

This dissertation has not been applied for the acquisition of an educational and scientific PhD in another school, university or scientific institute.

Chapter 1

Orthogonal Arrays

In this chapter we give some notations and properties of orthogonal arrays.

1.1 Orthogonal Arrays - definitions

Although the first notation for orthogonal arrays was more than fifty years ago, they are an active area today. They are related to Latin squares, Hadamard matrices, finite geometry and error-correcting codes. Although much has been done in this area, there are still many unsolved problems. Many researchers have found inspiration in this topic and new ones are being discovered all the time. The diversity in the background make and more difficult the contributions to this subject.

Definition 1.1.1. *[17] Let $\mathcal{A}$ be an alphabet of q symbols. An* ***Orthogonal Array*** $OA(M, n, q, t)$ ***of strength*** t ***with*** M ***rows,*** n ***columns*** $(n \geq t)$***, and*** q ***levels*** *is an $M \times n$ matrix (array) with entries from $\mathcal{A}$ so that every $M \times t$ submatrix contains each of the q^t possible t-tuples equally often as a row (say λ times).*

In 1940's in a series of papers C. R. Rao ([30, 31, 32]) introduced certain combinatorial arrangements with applications to statistics into an array structure, which has been later termed as an orthogonal array by Bush [9]. One of the first formal attempts to construct orthogonal array was undertaken by Seiden ([35, 36]) in 1954. He analysed the theory of Orthogonal array from the work done by Bose [1]. The book on Orthogonal arrays by Hedayat, Sloane and Stufken [17] has an important role in these theory. The interest of constructing orthogonal array is still alive [27, 45, 42].

Our task is to investigate structure of q-ary orthogonal array and hopefully to find some nonexistence result or some restriction of the structure.

Example 1.1.2. *The following array is an orthogonal array based on three levels, with strength two, of index unity, with nine runs and with four factors. It is an OA(9, 4, 3, 2). Where* $\lambda = \frac{M}{q^t} = 1$

$$\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 2 & 2 & 2 & 0 \\ 0 & 1 & 2 & 1 \\ 1 & 2 & 0 & 1 \\ 2 & 0 & 1 & 1 \\ 0 & 2 & 1 & 2 \\ 1 & 0 & 2 & 2 \\ 2 & 1 & 0 & 2 \end{array}$$

Let us pick any two columns, combination of symbols

$$(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)(2,0),(2,1),(2,2),$$

which appers the same number of times, exactly one, in each pair of columns of the OA. That's the property that makes it an orthogonal array.

As already mentioned, the main applications of orthogonal arrays are in planing experiments. We explain the example in other point of view. The number of rows (M) represent the number of runs in the experiment. The columns (factors - n) of the orthogonal array correspond to the different variables whose effects are being analyzed.

We consider coffee, sugar, milk, cream as the factors (or variables). In our example we have 4 columns. Which means we can vary the levels to these different variables. As a result we get various coffees - coffee, cappucino, turkish coffee, late coffee (the runs).

	coffee	sugar	milk	cream
cappucino	1	1	1	0
coffee	1	0	0	0

So we make different coffees or experiments if we put different quantities of each factor.

There are two main problems in the ares of the orthogonal array, i.e.

i) For fixed number of columns (factors) n, number of levels q and strength t, the problem is to find the smallest possible number of rows of the orthogonal array.

ii) For a given number of runs, to know the largest number of columns that can be construct an orthogonal array.

Definition 1.1.3. *[17] Orthogonal array without repeated rows is called* ***simple****.*

Definition 1.1.4. *[17] Let q be a prime power. An $OA(M, n, q, t)$ is said to be* ***linear*** *if it is simple and its rows form an linear space over $GF(q)$.*

Definition 1.1.5. *[17] A* **mixed orthogonal array** *$OA(M, n, q_1^{n_1} q_2^{n_2} ... q_v^{n_v}, t)$ is an array of size $M \times n$, where $n = n_1 + n_2 + ... + n_v$ is the total number of factors, in which the first n_1 columns have symbols from $0, 1, ..., q_1 - 1$, the next n_2 columns have symbols from $0, 1, ..., q_2 - 1$, and so on, with the property that in any $M \times t$ subarray every possible t-tuple occurs an equal number of times as a row.*

Example 1.1.6. *[17] A mixed orthogonal array that in fact is an $OA(8, 5, 4, 2)$ or $OA(8, 5, 4^1 2^4, 2)$, as we see the first column has three levels and the next four columns have two levels.*

0	0	0	0	0
0	1	1	1	1
1	0	1	0	1
1	1	0	1	0
2	0	0	1	1
2	1	1	0	0
3	0	1	1	0
3	1	0	0	1

1.2 Basic Properties

In this section we present some basic definitions and properties of orthogonal arrays which are important for our investigation.

Proposition 1.2.1. *[17] For an $OA(M, n, q, t)$ the following properties hold*

(i) Remind that the parameters of an orthogonal array satisfy the equality $\lambda = \frac{M}{q^t}$

(ii) A permutation of the symbols (levels q) of any factor (column n) in an $OA(M, n, q, t)$ results in orthogonal array with the same parameters.

(iii) A permutation of the runs or factors (columns n) in an $OA(M, n, q, t)$ results in orthogonal array with the same parameters.

(iv) Any $M \times k$ sub-array of $OA(M, n, q, t)$ is an $OA(M, k, q, t')$, where $t' = \min\{t, k\}$.

(v) If $A = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}$ is an $OA(M, n, q, t)$, where A_1 itself is an $OA(M_1, n, q, t_1)$, then A_2 is an $OA(M - M_1,\ n,\ q,\ t_2)$ with $t_2 \geq \min\{t, t_1\}$.

Proof. (v) If $t_1 \geq t$ then A_1 has strength t, thus in any t columns any $t-$tuple appears multiple of q^t times. But then the same has to be true for the $A_2 = A/A_1$, i.e., the strength of A_2 is at least t. Similarly if $t_1 < t$ then A_2 has strength at least t_1. □

Proposition 1.2.2. *[17] If A_i is $OA(M_i, n, q, t_i), \quad i = 1, \ldots, m, \quad$ then*

$$A = \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_m \end{bmatrix}$$

is $OA(M, n, q, t)$ with $M = M_1 + M_2 + \cdots + M_m$ and strength is t for some $t \geq \min\{t_1, t_2, \ldots, t_m\}$. Further, when $m = s$ and each A_i is an $OA(M, n, q, t)$ after appending a 1 to each row of A_1, a 2 to each row of A_2, and so on we obtain an $OA(qM, n + 1, q, t)$.

Definition 1.2.3. *[17] Two orthogonal arrays is said to be **isomorphic** if one can be obtained from the other*

(i) by a sequence of permutations of its rows (M),

(ii) by a sequence of permutations of its columns (n),

(iii) by a sequence of permutations of its symbols of each column.

Example 1.2.4. *The following $OA(8, 4, 2, 3)$ are isomorphic.*

1	0	0	0
0	1	0	0
0	0	1	0
0	0	0	1
0	1	1	1
1	0	1	1
1	1	0	1
1	1	1	0

0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

There are other similar results for some mixed orthogonal arrays (see for instance [17] and [29]).

Definition 1.2.5. *[17] Two orthogonal arrays are said to be* ***statistically equivalent*** *if one can be obtained from the other only by a permutation of the runs.*

So, in the Example 1.2.4, two orthogonal arrays are not statistically equivalent.

1.3 Orthogonal arrays and their relations to codes

In this section we give same basic properties for error-correcting codes and discuss their relation with orthogonal arrays. This section is based on the books [28] and [17].

1.3.1 Codes - definitions and properties

The theory of error-correcting codes began in the late 1940's by Shannon ([38, 39]).

Let the alphabet $\mathcal{A}$ be the finite field $GF(q)$, when q is a prime power (sometimes $\mathcal{A} = \mathbb{Z}_q$ be the additive commutative ring with unity of integers modulo q). The use of finite field $GF(q)$ as alphabet enables results from coding theory to be drawn in for solving problems concerning orthogonal arrays.

Hamming distance $d(\mathbf{x}, \mathbf{y})$ between two vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathcal{A}^n$, where $\mid \mathcal{A} \mid = q = p^m$ is the number of coordinates in which they differ:

$$d(\mathbf{x}, \mathbf{y}) \stackrel{def}{=} |\{i | x_i \neq y_i\}|.$$

Theorem 1.3.1. *([28]) The distance function* $d(\mathbf{x}, \mathbf{y})$ *satisfies the following four properties*

1. *(non-negativity)* $d(\mathbf{x}, \mathbf{y}) \geq 0$ *, for every* $x, y \in \mathcal{A}^n$*,*
2. $d(\mathbf{x}, \mathbf{y}) = 0$ *if and only if x=y,*
3. *(symmetry)* $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$*, for every* $x, y \in \mathcal{A}^n$*,*
4. *(triangle inequality)* $d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$*, for every* $x, y, z \in \mathcal{A}^n$*.*

The **Hamming weight** $wt(\mathbf{x})$ of a vector $\mathbf{x} \in \mathcal{A}^n$ is the number of non-zero coordinates in $\mathbf{x}$. Clearly, $wt(\mathbf{x}) = d(\mathbf{x}, 0)$, where $\mathbf{0}$ is all zero vector.

Theorem 1.3.2. *([28]) If* $\mathbf{x}, \mathbf{y} \in \mathcal{A}^n$ *then* $d(\mathbf{x}, \mathbf{y}) = wt(x - y)$.

Definition 1.3.3. *([28])* ***Linear*** $[n, k]$***-code*** *over* $\mathcal{A}$ *or* $[n, k]_q$*-code is called any* k*-dimentional linear subspace* C *of* $\mathcal{A}^n$*. The elements of* C *are called* ***codewords****.*

The **minimum distance** of a code C is the smallest distance between distinct codewords i.e.

$$d(C) = \min \{d(\mathbf{x}, \mathbf{y}) \mid x, y \in C, x \neq y\}.$$

Theorem 1.3.4. *([28]) If* C *is a linear code, the minimum distance* d *is the same as the minimum weight of the nonzero codewords of* C*.*

Definition 1.3.5. *([28]) A linear code over* $\mathcal{A}$ *with length* n*, dimention* k *and minimum distance* d *we call* $[n, k, d]_q$*-code.*

Codes over the fields of orders 2, 3 and 4 are called binary, ternary and quaternary etc. codes, respectively.

In the linear space $\mathcal{A}^n$ is defined the scalar product in usual way as

$$(x, y) = x_1y_1 + x_2y_2 + ... + x_ny_n,$$

where $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ are vectors in $\mathcal{A}^n$. Two vectors x, y are orthogonal if their scalar product is zero, i.e. $(x, y) = 0$.

Definition 1.3.6. *The set of all vectors of* $\mathcal{A}^n$ *orthogonal to every codeword of* C *is called an* ***dual code****, named* $C^\perp$*, i.e.*

$$C^\perp = \{x \in \mathcal{A}^n | (x, y) = 0 \ \forall y \in C\}.$$

A **generator matrix** for an $[n,\ k]_q$ code C is any $k \times n$ matrix G whose rows form a basis for C. A code has many generator matrices. If the generator matrices is in the form $[I_k, A]$ where I_k is the $k \times k$ identity matrix, then we say that the generator matrix is in the **standart form**. The generator matrix G of $[n, k]_q$ code C is simply a matrix whose rows are independent and span the code.

For any set of k independent columns of a generator matrix G, the corresponding set of coordinates forms an **information set** for C.

Definition 1.3.7. *([28]) A matrix,* H*, is called* ***a parity check*** *matrix for a linear code if and only if for every codeword* c *in* C*,* $Hc^T = 0$*.*

Theorem 1.3.8. *([28]) If* $G = \left[\begin{array}{c|c} I_k & A \end{array}\right]$ *is a generator matrix for the* $[n, k]$ *code* C *in standart form then* $H = \left[\begin{array}{c|c} -A^T & I_n - k \end{array}\right]$ *is a parity check matrix.*

Theorem 1.3.9. *([17]) Let C be a $[n,k]_q$ linear code. Then*

$$\begin{aligned} C^{\perp} &= \left\{x \in F_q^n \mid \ x \cdot c_i = 0 \text{ for all } c_i \in C\right\} \\ &= \left\{x \in F_q^n \mid xG^{\perp} = 0\right\} \\ &= \left\{x \in F_q^n \mid \ Gx^{\perp} = 0\right\} \end{aligned}$$

(i) the dual code $C^{\perp}$ has length n, dimension $n-k$, and the minimal distance $d^{\perp}$, i.e $C^{\perp}$ is an $[n, n-k]_q$ code ,

(ii) a generator matrix for C is a parity check matrix for $C^{\perp}$, a parity check matrix for C is a generator matrix for $C^{\perp}$,

(iii) $(C^{\perp})^{\perp} = C$.

Definition 1.3.10. *A code C is called **self-orthogonal** if $C \subseteq C^{\perp}$ and **self–dual** if $C = C^{\perp}$.*

The length n of a self-dual code is even and the dimension is $n/2$. We denote by $d^{\perp}$ the **dual distance** of C. So, if C is $[n,k]_q$-code and has dimention $\dim C = k$ then $C^{\perp}$ is $[n, n-k]_q$ -code and its dimention is $\dim C^{\perp} = n-k$. It is clear that $(C^{\perp})^{\perp} = C$ and $\dim C + \dim C^{\perp} = n$.

Theorem 1.3.11. *Let C is a linear $[n,k]_q$-code with parity check matrix H. Minimum distance of C is d if any $d-1$ columns in H are linearly independent and in H exists d linear dependent columns.*

As a result of this theorem, for linear codes, the minimum distance is also called the minimum weight of the code. Let A_i also denoted $A_i(C)$, be the number of codewords of weight i in C. The set of A_i for $0 \leq i \leq n$ is called **distance distribution** of C, i.e.

$$A_i \stackrel{def}{=} \frac{1}{|C|} \left|\{(\mathbf{x}, \mathbf{y}) \in C^2 \mid d(\mathbf{x}, \mathbf{y}) = i\}\right|.$$

And by Delsarte inequalities [13] we have $A_0 = ... = A_{d-1} = 0$ where $d = d(C)$ is the minimum distance of C. Note that, $t = d^{\perp} - 1$ is the maxmimum strength of the orthogonal array formed by codewords.[1].

1.3.2 Orthogonals arrays and codes

Now, we give the relationship between parameters of orthogonal arrays and codes. We can use the codewords in an error-correcting code as the runs of an orthogonal

array, or conversely we can consider the runs of an orthogonal array as constructing a code.

Let us considered the alphabet $\mathcal{A} = GF(q)$, where $q = p^e$ is a prime power. Then the set of the distinct rows of any orthogonal array $OA(M, n, q, t)$ can be considered as a q-ary code, in general nonlinear, of block length n having $\leq M$ codewords. If $OA(M, n, q, t)$ is linear then $M = q^k$ for some $t \leq k \leq n$.

Theorem 1.3.12. *([17]) The orthogonal array associated with a code is linear if and only if the code is linear.*

Proof. This follows immediately from the definitions of linearity of the orthogonal arrays and the codes. □

Theorem 1.3.13. *Let C be a $M \times n$ matrix whose rows form a linear subspace of $\mathcal{A}^n$, $\mathcal{A} = GF(q)$. If any t columns of C are linearly independent over $\mathcal{A}$, then C is an $OA(M, n, q, t)$.*

Proof. Suppose $M = q^k$, $t \leq k \leq n$. Let $\mathbf{G}$ be $k \times n$ submatrix of C with rank k. Then any row of C can be presented as $\mathbf{uG}$, where $\mathbf{u} \in \mathcal{A}^k$. Choose t columns of C and let $\mathbf{G}_1$ be the $k \times t$ submatrix of $\mathbf{G}$ corresponding to the chosen columns. Obviously $\operatorname{rank} \mathbf{G}_1 = t$. Hence the restriction of rows of C to the chosen columns are linear combinations of the rows of $\mathbf{G}_1$ and any t-tuple is repeated q^{k-t} times. □

The following theorem shows how linear codes and linear orthogonal arrays are related.

Theorem 1.3.14. *([13])*

(i) If C is an $[n, k, d]_q$ linear code then its dual code $C^\perp$ is $OA(q^{n-k}, n, q, d-1)$ with index $\lambda = q^{n-k-d+1}$.

(ii) The code C itself is an $OA(q^k, n, q, d^\perp - 1)$, where $d^\perp$ is the minimal distance of $C^\perp$.

Example 1.3.15. *Let C be the $[4, 2, 3]_3$ Hamming code over $\mathbb{Z}_3$ given by a parity check matrix*

$$\mathbf{H} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix}.$$

The dual code $C^\perp$ is a $[4, 2, 3]_3$ code generated by the rows of $\mathbf{H}$. Below $C^\perp$ and permutated one by $\sigma = (012)$ are given

0	0	0	0		1	1	1	1
0	1	1	1		1	2	2	2
0	2	2	2		1	0	0	0
1	0	1	2		2	1	2	0
2	0	2	1		0	1	0	2
1	1	2	0		2	2	0	1
2	2	1	0		0	0	2	1
1	2	0	1		2	0	1	2
2	1	0	2		0	2	1	0

It is easy to check that they both are $OA(9, 4, 3, 2)$. Indeed C is self dual, that is, $C = C^{\perp}$. The generator matrix of C is

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

If C contains M codewords then we say that it is a **code of length n, size M and minimal distance d over an alphabet of size** q, or simply a $(n, M, d)_q$ code. The following theorem shows the relationship between codes and orthogonal arrays.

Theorem 1.3.16. *[13]*

(i) If C is an $(n, M, d)_q$-ary code with dual distance $d^{\perp}$ then the corresponding orthogonal array is an $OA(M, n, q, d^{\perp} - 1)$.

(ii) Conversely, the code corresponding to an $OA(M, n, q, \tau)$ is $(n, M, d)_q$-ary code with dual distance $d^{\perp} \geq \tau + 1$. If the OA has strength τ but not $\tau + 1$, $d^{\perp}$ is precisely $\tau + 1$.

The correspondence between orthogonal arrays and codes is summarized in the following table:

Orthogonal arrays $OA(M, n, q, \tau)$		**Codes** $(n, M, d)_q$
number of levels	q	alphabet size
number of factors	n	length of code
number of runs	M	number of codewords
strength	$\tau = d^{\perp} - 1$	minimal distance of dual

This could be can be outlined in:

1. a good error-correcting code is a large set of vectors of given length whose distance apart is as large as possible.

2. a good orthogonal array is a small set of vectors of given length whose dual distance is as large as possible.

Coding theory has much to contribute to orthogonal arrays.

(i) **Direct construction** of OA from codes, simply by taking the codewords as the runs of the array.

(ii) **New general construction techniques** for OA that are modifications of existing construction techniques for codes (for example, methods for combining two or more orthogonal arrays to form a new array)

(iii) **Bounds** on the minimal number of runs in an OA, obtained by forming a code from the runs of the array and then using bounds from coding theory. The most important of these bounds is Delsarte's (1973) linear programming bound.

1.4 Krawtchouk polynomial

Krawtchouk polynomials are introduced in 1929 by Ukrainian mathematician Krawtchouk as a generalization of Hermite polynomials and they play an important role in coding theory and are also useful in graph theory and number theory (see, e.g., [22, 15], [19], [41], and [25]). .

1.4.1 Orthogonal polynomials

Let ***Euclidean space*** E be a linear space over the field of real numbers $\mathbb{R}$ supplied with ***scalar product***, i.e., supplied with a map

$$\langle , \rangle : \left| \begin{array}{c} E^2 \longrightarrow \mathbb{R} \\ (\mathbf{x}, \mathbf{y}) \longrightarrow \langle \mathbf{x}, \mathbf{y} \rangle \end{array} \right.$$

with the properties

1. $\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle$

2. $\langle \lambda \mathbf{x} + \mu \mathbf{y}, \mathbf{z} \rangle = \lambda \langle \mathbf{x}, \mathbf{z} \rangle + \mu \langle \mathbf{y}, \mathbf{z} \rangle$ (bilinearity);

3. $\langle \mathbf{x}, \mathbf{x} \rangle > 0$ for any $\mathbf{x} \neq \mathbf{0}$;

The ***norm*** of $\mathbf{x}$ is $||\mathbf{x}|| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle}$.

Two nonzero vectors $\mathbf{x}, \mathbf{y}$ are called ***orthogonal***, denoted by $\mathbf{x} \perp \mathbf{y}$, if $\langle \mathbf{x}, \mathbf{y} \rangle = 0$. Any subset of pairwise orthogonal vectors of E (called ***orthogonal system***) is a set of linearly independent vectors. If $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ is an orthogonal system of vectors of E and $\mathbf{x} = \sum_{i=1}^{n} \lambda_i \mathbf{e}_i$, then this representation is unique and $\lambda_i = \dfrac{\langle \mathbf{x}, \mathbf{e}_i \rangle}{\langle \mathbf{e}_i, \mathbf{e}_i \rangle}$.

Let $E \subset \mathbb{R}[x]$ be the linear space of polynomials of degree up to n. It is easy to check that the bilinear map defined by

$$\langle f, g \rangle \stackrel{def}{=} \sum_{i=0}^{n} k_i f(x_i) g(x_i), \quad k_i \geq 0,$$

where $(x_0, x_1, \ldots, x_n) \in \mathbb{R}^{n+1}$ is a fixed $(n+1)$-tuple of different real numbers called ***approximation points***, satisfies the axioms for scalar product. Usually the ***weight vector*** $(k_0, k_1, \ldots, k_n)$ is chosen to satisfy $\sum_{i=0}^{n} k_i = 1$ in order to assure that the norm is 1.

In what is follow we give two examples of scalar products. Here is the first one.

Krawtchouk polynomials

Let $q \geq 2$ be integer, $(0, 1, \ldots, n)$ be the approximation points, and

$$\langle f, g \rangle \stackrel{def}{=} \frac{1}{q^n} \sum_{i=0}^{n} \binom{n}{i} (q-1)^i f(i) g(i). \tag{1.1}$$

The weight vector is

$$\frac{1}{q^n} \left(1, \ \binom{n}{1}(q-1), \ \ldots, \ \binom{n}{n}(q-1)^n \right)$$

and satisfies

$$\sum_{i=0}^{n} \binom{n}{i} \frac{(q-1)^i}{q^n} = 1.$$

Definition 1.4.1. ***Krawtchouk polynomial*** *is a polynomial defined by*

$$K_k(x;\, n, q) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j} (q-1)^{k-j}, \quad k = 0, 1 \ldots n.$$

Usually n and q have already been fixed or their values are known from context. Hence for simplicity we often omit n and q and write only $K_k(x)$.

The Krawtchouk polynomial $K_k(x;\, n, q)$ is a polynomial of degree k in x with leading coefficient $(-q)^k/k!$. Here are the first three polynomials:

$$\begin{aligned}
K_0(x) &= 1;\\
K_1(x) &= -qx + n(q-1);\\
K_2(x) &= \frac{1}{2}\Big[q^2x^2 - \big((2n-1)(q-1)+1\big)x + n(n-1)(q-1)^2\Big].
\end{aligned}$$

The generating function of Krawtchouk polynomials is

$$\sum_{k=0}^{n} K_k(x;\, n, q)z^k = \Big(1 + (q-1)z\Big)^{n-x}(1-z)^x. \tag{1.2}$$

Proposition 1.4.2. *Krawtchouk polynomials satisfy the relations*

$$(q-1)^i\binom{n}{i}K_k(i) = (q-1)^k\binom{n}{k}K_i(k). \tag{1.3}$$

Proof. It is easy to check that

$$\binom{n}{i}\binom{i}{j}\binom{n-i}{k-j} = \binom{n}{k}\binom{k}{j}\binom{n-k}{i-j}.$$

Hence

$$\begin{aligned}
(q-1)^i\binom{n}{i}K_k(i) &= \sum_{j=0}^{n}(-1)^j\binom{n}{i}\binom{i}{j}\binom{n-i}{k-j}(q-1)^{k-j+i}\\
&= \sum_{j=0}^{n}(-1)^j\binom{n}{k}\binom{k}{j}\binom{n-k}{i-j}(q-1)^{k-j+i}\\
&= \binom{n}{k}(q-1)^k\sum_{j=0}^{n}(-1)^j\binom{k}{j}\binom{n-k}{i-j}(q-1)^{i-j}\\
&= \binom{n}{k}(q-1)^k K_i(k).
\end{aligned}$$

□

Lemma 1.4.3. *Krawtchouk polynomials $K_0(x), K_1(x), \ldots, K_n(x)$ form an orthogonal system regarding to the scalar product (1.1), namely*

$$\langle K_k, K_l\rangle = \frac{1}{q^n}\sum_{i=0}^{n}\binom{n}{i}(q-1)^i K_k(i)K_l(i) = \binom{n}{k}(q-1)^k\,\delta_{kl} \tag{1.4}$$

for $k, l = 0, 1, \ldots, n$, where δ_{kl} is Kronecker delta.

Proof. Let $L_{k,l}$ and $R_{k,l}$ be the left and right sides of the above relation, respectively. Consider their generating functions

$$\sum_{k=0}^{n}\sum_{k=0}^{n} L_{k,l}x^k y^l \qquad \text{and} \qquad \sum_{k=0}^{n}\sum_{k=0}^{n} R_{k,l}x^k y^l.$$

Obviously $L_{k,l} = R_{k,l}$ for any k, l if and only if their generating function are equal.

Using (1.2) we obtain

$$\begin{aligned}
\sum_{k=0}^{n}\sum_{l=0}^{n} L_{k,l}x^k y^l &= \\
&= \frac{1}{q^n}\sum_{i=0}^{n}\binom{n}{i}(q-1)^i \sum_{k=0}^{n}\sum_{l=0}^{n} K_k(i)K_l(i)x^k y^l \\
&= \frac{1}{q^n}\sum_{i=0}^{n}\binom{n}{i}(q-1)^i \left(\sum_{k=0}^{n} K_k(i)x^k\right)\left(\sum_{l=0}^{n} K_l(i)y^l\right) \\
&= \frac{1}{q^n}\sum_{i=0}^{n}\binom{n}{i}(q-1)^i \Big(1+(q-1)x\Big)^{n-i}(1-x)^i \Big(1+(q-1)y\Big)^{n-i}(1-y)^i \\
&= \frac{1}{q^n}\Big[\big(1+(q-1)x\big)\big(1+(q-1)y\big) + (q-1)(1-x)(1-y)\Big]^n \\
&= \frac{1}{q^n}\Big(q+q(q-1)xy\Big)^n \\
&= \Big(1+(q-1)xy\Big)^n.
\end{aligned}$$

On the other side we have

$$\begin{aligned}
\sum_{k=0}^{n}\sum_{l=0}^{n} R_{k,l}x^k y^l &= \sum_{k=0}^{n}\sum_{l=0}^{n}\binom{n}{k}(q-1)^k x^k y^l\,\delta_{kl} \\
&= \sum_{k=0}^{n}\binom{n}{k}(q-1)^k x^k y^k \\
&= \Big(1+(q-1)xy\Big)^n.
\end{aligned}$$

Since the two sums are equal, the assertion is true. □

Now using (1.3) to express $K_l(i)$ by $K_i(l)$ in (1.4) we obtain the so called *second orthogonality relation.*

Corollary 1.4.4.

$$\sum_{i=0}^{n} K_k(i)K_i(l) = q^n\delta_{kl} \tag{1.5}$$

Theorem 1.4.5. *For any polynomial $f(x) \in \mathbb{R}[x]$ of degree $\leq n$ there is a unique expansion*

$$f(x) = \sum_{k=0}^{n} f_k K_k(x), \qquad \textit{where}$$

$$f_k = \frac{1}{q^n \binom{n}{k} (q-1)^k} \sum_{i=0}^{n} \binom{n}{i} (q-1)^i f(i) K_k(i) = \frac{1}{q^n} \sum_{i=0}^{n} f(i) K_i(k).$$

Proof. $\{K_0(x), K_1(x), \ldots, K_n(x)\}$ form an orthogonal basis in the the space of polynomials of degree $\leq n$. Hence the expansion of $f(x)$ exists, it is unique, and

$$f_k = \frac{\langle f(x), K_k(x) \rangle}{\langle K_k(x), K_k(x) \rangle},$$

which gives the first equality. The second equality follows from (1.3). □

1.4.2 Properties

Generating function (1.2) of Krawtchouk polynomials enables many important their properties to be derived. The next propositions illustrate this fact.

Proposition 1.4.6. *Krawtchouk polynomials satisfies the following relations*

$$(a) \quad K_k(x) = \sum_{\nu=0}^{k} (-1)^{k-\nu} q^\nu \binom{n-\nu}{k-\nu} \binom{n-x}{\nu} \tag{1.6}$$

$$(b) \quad K_k(x) = \sum_{\nu=0}^{k} (-q)^\nu \binom{n-\nu}{k-\nu} \binom{x}{\nu} (q-1)^{k-\nu} \tag{1.7}$$

Proof. (a)

$$\begin{aligned}
(1+(q-1)z)^{n-x}(1-z)^x &= ((1-z)+qz)^{n-x}(1-z)^x = \\
&= \left[\sum_{\nu=0}^{n-x} \binom{n-x}{\nu} (1-z)^{n-x-\nu} q^\nu z^\nu\right] (1-z)^x \\
&= \sum_{\nu=0}^{n-x} \binom{n-x}{\nu} (1-z)^{n-\nu} q^\nu z^\nu \\
&= \sum_{\nu=0}^{n-x} \binom{n-x}{\nu} \left(\sum_{\mu=0}^{n-\nu} (-1)^\mu \binom{n-\nu}{\mu} z^\mu\right) q^\nu z^\nu \\
&= \sum_{\nu=0}^{n-x} \sum_{\mu=0}^{n-\nu} (-1)^\mu \binom{n-x}{\nu} \binom{n-\nu}{\mu} q^\nu z^{\nu+\mu}
\end{aligned}$$

he coefficient at z^k in the left side is $K_k(x)$ while in the right side is the sum of coefficients at $z^{\nu+\mu}$ when $\nu+\mu=k$, i.e., $\mu=k-\nu$.

(b)

$$\begin{aligned}(1+(q-1)z)^{n-x}(1-z)^x &= (1+(q-1)z)^{n-x}[(1+(q-1)z)-qz]^x = \\ &= (1+(q-1)z)^{n-x}\sum_{\nu=0}^{x}\binom{x}{\nu}(-q)^\nu(1+(q-1)z)^{x-\nu}z^\nu \\ &= \sum_{\nu=0}^{x}\binom{x}{\nu}(-q)^\nu(1+(q-1)z)^{n-\nu}z^\nu \\ &= \sum_{\nu=0}^{x}\binom{x}{\nu}(-q)^\nu\left(\sum_{\mu=0}^{n-\nu}\binom{n-\nu}{\mu}(q-1)^\mu z^\mu\right)z^\nu \\ &= \sum_{\nu=0}^{x}\sum_{\mu=0}^{n-\nu}\binom{x}{\nu}\binom{n-\nu}{\mu}(-q)^\nu(q-1)^\mu z^{\mu+\nu}.\end{aligned}$$

Similarly, the coefficient at z^k in the right side is the sum of coefficients at $z^{\nu+\mu}$ when $\nu+\mu=k$, i.e., $\mu=k-\nu$. □

Proposition 1.4.7. *The sequence of Krawtchouk polynomials satisfies the recurrence relation*

$$kK_k(x)=\big(-qx+(n-k+1)(q-1)+k-1\big)K_{k-1}(x)-(q-1)(n-k+2)K_{k-2}(x), \quad (1.8)$$

for $k=2,3,\ldots,n$.

Proof. Differentiating both sides of (1.2) with respect to z we obtain

$$\sum_{k=0}^{n}kK_k(x)z^{k-1}=\Big(1+(q-1)z\Big)^{n-x-1}(1-z)^{x-1}\Big[(n-x)(q-1)(1-z)-x(1+(q-1)z)\Big]$$

Multiplying both sides by $\big(1+(q-1)z\big)(1-z)=1+(q-2)z-(q-1)z^2$ we have

$$\begin{aligned}&\sum_{k=0}^{n}kK_k(x)z^{k-1}+(q-2)\sum_{k=0}^{n}kK_k(x)z^k-(q-1)\sum_{k=0}^{n}kK_k(x)z^{k+1}= \\ &\qquad=\Big[\big(-qx+n(q-1)\big)-\big((n-x)(q-1)+x(q-1)\big)z\Big]\sum_{k=0}^{n}K_k(x)z^k \\ &\qquad=\big(-qx+n(q-1)\big)\sum_{k=0}^{n}K_k(x)z^k-n(q-1)\sum_{k=0}^{n}K_k(x)z^{k+1}\end{aligned}$$

Comparing the coefficients at z^{k-1} we obtain

$$\begin{aligned} kK_k(x) + (q-2)(k-1)K_{k-1}(x) - (q-1)(k-2)K_{k-2}(x) = \\ = \big(-qx + n(q-1)\big)K_{k-1}(x) - n(q-1)K_{k-2}(x) \end{aligned}$$

Therefore

$$kK_k(x) = \Big(-qx + (n-k+1)(q-1) + k - 1 \Big)K_{k-1}(x) - (q-1)(n-k+2)K_{k-2}(x).$$

□

In the sequel we will often use the matrices

Definition 1.4.8. ***Krawtchouk matrix*** *is referred to be the $n \times n$ matrix*

$$\mathbf{K} = \big(K_i(j)\big), \qquad i, j = 1, 2, \ldots, n.$$

The $(n+1) \times (n+1)$ matrix $\widehat{\mathbf{K}}$ obtained from $\mathbf{K}$ by adding all-ones vector as a first row and $\mathbf{B} = (K_0(0), K_1(0), K_2(0), \ldots, K_n(0))^\tau$ as a first column is called the ***extended Krawtchouk matrix****.*

The second orthogonal relation (1.5) gives

$$\widehat{\mathbf{K}}\widehat{\mathbf{K}} = q^n \mathbf{I}_n.$$

It is easy to check that

$$K_k(0) = \binom{n}{k}(q-1)^k, \quad K_k(n) = (-1)^k \binom{n}{k}, \quad K_n(i) = (-1)^i (q-1)^{n-i} \tag{1.9}$$

Matrix $\mathbf{K}$ can be computed recursively using the following relation

Proposition 1.4.9. *The values $K_i(j), i, j = 1, 2, \ldots, n$ satisfy the recurrence relation*

$$K_k(j) = K_k(j-1) - \big[K_{k-1}(j-1) + (q-1)K_{k-1}(j)\big] \qquad k, j = 1, 2, \ldots, n. \tag{1.10}$$

Proof. Replacing x by $(x-1)$ in (1.2) we have

$$\sum_{k=0}^{n} K_k(x-1)z^k = \big(1 + (q-1)z\big)^{n-x+1}(1-z)^{x-1}.$$

Now we multiply both sides with $(1-z)$:

$$\begin{aligned}\sum_{k=0}^{n} K_k(x-1)z^k - \sum_{k=0}^{n} K_k(x-1)z^{k+1} &= \big(1+(q-1)z\big)\big(1+(q-1)z\big)^{n-x}(1-z)^x \\ &= \big(1+(q-1)z\big)\sum_{k=0}^{n} K_k(x)z^k \\ &= \sum_{k=0}^{n} K_k(x)z^k + (q-1)\sum_{k=0}^{n} K_k(x)z^{k+1}\end{aligned}$$

Comparing the coefficients at z^k we obtained

$$K_k(x-1) - K_{k-1}(x-1) = K_k(x) + (q-1)K_{k-1}(x-1),$$

which gives (1.10). □

Besides the general properties of orthogonal polynomials (e.g. [41]) they posses many other interesting properties. We give several of them in the theorem below.

Theorem 1.4.10. *The following relations hold:*

(i) $K_k(x;\, n) = (q-1)K_{k-1}(x;\, n-1) + K_k(x;\, n-1)$;

(ii) $(q-1)K_k(x;\, n) + K_k(x-1;\, n) = qK_k(x-1;\, n-1)$;

(iii) $\sum_{k=0}^{n} \binom{n-k}{n-j} K_k(x) = q^j \binom{n-x}{j}$;

(iv) $\sum_{k=0}^{m} K_k(x;n) = K_m(x-1;n-1)$.

1.4.3 Normalized Krawtchouk polynomials

Let

$$t_i = 1 - \frac{2i}{n},\ i = 0, 1, \ldots, n. \tag{1.11}$$

Hence $1 = t_0 > t_1 > \cdots > t_n = -1$ and $t_i = -t_{n-i}$.

Definition 1.4.11. ***Normalized Krawtchouk polynomials*** *are defined by*

$$\begin{aligned}Q_k(x) &\stackrel{def}{=} \frac{1}{K_k(0)} K_k\left(\frac{n}{2}(1-x)\right) \\ &= \frac{1}{\binom{n}{k}(q-1)^k} K_k\left(\frac{n}{2}(1-x)\right).\end{aligned}$$

A straightforward computations show that $Q_k(1) = 1$ and

$$K_k(i) = \binom{n}{k}(q-1)^k Q_k(t_i), \quad i = 0, 1, \ldots, n. \tag{1.12}$$

Now using (1.3) we obtain that

$$Q_k(t_i) = Q_i(t_k).$$

Replacing $K_k(i)$ in the orthogonality relations (1.4) and (1.5) we obtain respectively

$$\sum_{i=0}^{n} \binom{n}{i}(q-1)^i Q_k(t_i)Q_l(t_i) = \frac{q^n}{\binom{n}{k}(q-1)^k}\delta_{kl} \tag{1.13}$$

$$\sum_{i=0}^{n} \binom{n}{i}(q-1)^i Q_k(t_i)Q_i(t_l) = \frac{q^n}{\binom{n}{k}(q-1)^k}\delta_{kl} \tag{1.14}$$

The equality (1.13) shows that the polynomials $\{Q_k(x)\}$ are pairwise orthogonal polynomials in respect to the scalar product defined by

$$< f(x), g(x) > \stackrel{def}{=} \frac{1}{q^n}\sum_{i=0}^{n} \binom{n}{i}(q-1)^i f(t_i)g(t_i). \tag{1.15}$$

This definition differs from (1.1) only in the set of approximation points.

Relations (1.13), (1.14), and $Q_0(x) = 1$ give

$$\sum_{i=0}^{n} \binom{n}{i}(q-1)^i Q_k(t_i) = \sum_{i=0}^{n} \binom{n}{i}(q-1)^i Q_i(t_k) = \begin{cases} 0, & k > 0 \\ q^n, & k = 0 \end{cases} \tag{1.16}$$

Theorem 1.4.12. *For any polynomial $f(x) \in \mathbb{R}[x]$ of degree $\leq n$ there is a unique expansion*

$$f(x) = \sum_{k=0}^{n} f_k Q_k(x), \qquad \textit{where}$$

$$f_k = \frac{\binom{n}{k}(q-1)^k}{q^n}\sum_{i=0}^{n} \binom{n}{i}(q-1)^i f(t_i)Q_k(t_i), \quad k = 0, 1, \ldots, n. \tag{1.17}$$

Proof. Polynomials $\{Q_k(x)\},\ u = 0, \ldots, n$, form an orthogonal basis, thus any polynomial has unique expansion and

$$f_k = \frac{\langle f(x), Q_k(x)\rangle}{\langle Q_k(x,)Q_k(x)\rangle}.$$

Now we use (1.15) to prove the assertion. □

We illustrate the applications of the above theorem by giving an explicit formula for a sequence of constants which some researchers in the area of orthogonal arrays use. Using (1.17) and $Q_0(t) = 1$ we obtain

Corollary 1.4.13. *Let b_k denote the first coefficient in the Q-expansion of x^k, that is, $x^k = b_k + \sum_{j=1}^{k} a_j Q_j(t)$. Then*

$$b_k = \frac{1}{q^n} \sum_{i=0}^{n} \binom{n}{i} (q-1)^i \, t_i^k, \quad k = 0, 1, \ldots, n. \tag{1.18}$$

In partial

$$b_0 = 1, \quad b_1 = \frac{2-q}{q}, \quad b_2 = 1 - \frac{4(n-1)(q-1)}{nq^2}.$$

1.4.4 Additive characters

Definition 1.4.14. ***Character*** *χ of a finite group G with order $n = |G|$ is homomorphism of G into the multiplicative group of complex number $\mathbb{C}^*$. It is called* ***additive*** *character if G is additive group and* ***multiplicative*** *character if G is multiplicative.*
The term ***additive character of a ring or a field*** *means character of its additive group. ([18, 37])*

Since the order of any $g \in G$ divides n we have

$$\chi(g)^n = \chi(ng) = \chi(0) = 1.$$

Thus, any character χ of G is homomorphism into $\mathbb{C}_n$, the group of n-roots of unity. For example any character of the finite field $\mathbb{F}_q$, $q = p^e$, with characteristic p is homomorphism into $\mathbb{C}_p$, since $pa = 0$ for any $a \in \mathbb{F}_q$. Any character of $\mathbb{Z}_q$ is homomorphism into $\mathbb{C}_q$.

Characters of G form a multiplicative group isomorphic to G. Hence they can be indexed by the elements of G. We will not enter deeply inside theory of characters. We will only describe explicitly characters of $\mathbb{Z}_q$ and $\mathbb{F}_q$ and gives their properties.

The case $\mathcal{A} = \mathbb{Z}_q$, $q = p$.

Let $\xi \in \mathbb{C}$ be a primitive q-root of unity. The group of all additive characters of $\mathbb{Z}_q$ consists of all $\{\chi_a : \mathbb{Z}_q \to \mathbb{C}_q \mid a \in \mathbb{Z}_q\}$ defined by $\chi_a(x) = \xi^{ax}$, where $a, x \in \mathbb{Z}_q$.

It is easy to check that

$$\begin{aligned}
\chi_0(x) &= \chi_a(0) = 1,\\
\chi_a(x) &= \chi_x(a),\\
\chi_a(x+y) &= \chi_a(x)\chi_a(y),\\
\chi_a(-x) &= \chi_a(x)^{-1} = \overline{\chi_a(x)}
\end{aligned}$$

$$\sum_{x\in\mathbb{Z}_q}\chi_a(x) = \begin{cases} 0, & a\neq 0\\ q, & a=0\end{cases} \quad \text{or equivalently} \quad \sum_{x\in\mathbb{Z}_q^*}\chi_a(x) = \begin{cases} -1, & a\neq 0\\ q-1, & a=0\end{cases} \tag{1.19}$$

The case $\mathcal{A}=\mathbb{F}_q,\ q=p^e$.

Let $\xi\in\mathbb{C}$ be a primitive p-root of unity. $\mathbb{F}_q$ is a linear space with dimension e over $\mathbb{Z}_p$, thus, any element $x\in\mathbb{F}_q$ is uniquely represented by its coordinates $(x_1,\ldots,x_e)$ with respect to a fixed basis of $\mathbb{F}_q$ over $\mathbb{Z}_q$. Let $a\in\mathbb{F}_q$ has coordinates $(a_1,a_2,\ldots,a_e)$. The character χ_a is defined by

$$\chi_a(x) = \xi^{\langle a,x\rangle} = \xi^{a_1x_1+a_2x_2+\cdots+a_ex_e}.$$

Additive characters of $\mathcal{A}$ can be lifted to characters of the additive group of $\mathcal{A}^n$. We describe this process for $\mathcal{A}=\mathbb{Z}_q$ for concreteness, but everywhere $\mathbb{Z}_q$ can be replaced with $\mathbb{F}_q$ without any modification.

Definition 1.4.15. *For any $\mathbf{u}=(u_1,\ldots,u_n)\in\mathbb{Z}_q^n$ the map $\chi_{\mathbf{u}}:\mathbb{Z}_q^n\to\mathbb{C}_q$ define by*

$$\chi_{\mathbf{u}}(\mathbf{v}) = \xi^{<\mathbf{u},\mathbf{v}>} = \prod_{i=1}^{n}\chi_{u_i}(v_i),$$

where $\langle\mathbf{u},\mathbf{v}\rangle = u_1v_1+u_2v_2+\cdots+u_nv_n$ is the inner product of $\mathbf{u}$ and $\mathbf{v}$, is called ***an additive character*** *of $\mathbb{Z}_q^n$.*

It is straightforward to prove the following properties

$$\begin{aligned}
\chi_{\mathbf{0}}(\mathbf{u}) &= \chi_{\mathbf{u}}(\mathbf{0}) = 1,\\
\chi_{\mathbf{u}}(\mathbf{v}) &= \chi_{\mathbf{v}}(\mathbf{u}),\\
\chi_{\mathbf{u}}(\mathbf{v}+\mathbf{w}) &= \chi_{\mathbf{u}}(\mathbf{v})\chi_{\mathbf{u}}(\mathbf{w})\\
\chi_{\mathbf{u}}(-\mathbf{v}) &= \chi_{-\mathbf{u}}(\mathbf{v}) = \overline{\chi_{\mathbf{u}}(\mathbf{v})},
\end{aligned}$$

which assert that $\chi_{\mathbf{u}}$ are indeed additive characters of $\mathbb{Z}_q^n$.

Proposition 1.4.16. *For any* $\mathbf{u} \in \mathbb{Z}_q^n$

$$\sum_{\mathbf{v}\in\mathbb{Z}_q^n} \chi_{\mathbf{u}}(\mathbf{v}) = \begin{cases} 0, & \mathbf{u} \neq \mathbf{0} \\ q^n, & \mathbf{u} = \mathbf{0} \end{cases}$$

Proof. Let $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$.

$$\begin{aligned} \sum_{\mathbf{v}\in\mathbb{Z}_q^n} \chi_{\mathbf{u}}(\mathbf{v}) &= \sum_{\mathbf{v}\in\mathbb{Z}_q^n} \prod_{i=1}^{n} \chi_{u_i}(v_i) \\ &= \sum_{(v_1,\ldots,v_{n-1})\in\mathbb{Z}_q^{n-1}} \prod_{i=1}^{n-1} \chi_{u_i}(v_i) \left(\sum_{v_n\in\mathbb{Z}_q} \chi_{u_n}(v_n) \right) \\ &= \cdots \\ &= \left(\sum_{v\in\mathbb{Z}_q} \chi_{u_1}(v) \right) \left(\sum_{v\in\mathbb{Z}_q} \chi_{u_2}(v) \right) \cdots \left(\sum_{v\in\mathbb{Z}_q} \chi_{u_n}(v) \right) \end{aligned}$$

According to (1.19) if there is $u_i \neq 0$ then the i-th factor is zero, thus the product is zero. Otherwise all factors are equal to q, hence, the product is q^n. □

The following fundamental lemma is due to Ph. Delsarte [12, 14, 13].

Lemma 1.4.17. *Let* $\mathbf{u} \in \mathbb{Z}_q^n$ *be a fixed vector of weight* $wt(\mathbf{u}) = t$ *and* $W_k \subset \mathbb{Z}_q^n$ *be the subset of all vectors of weight* k*. Then*

$$\sum_{\mathbf{v}\in W_k} \chi_{\mathbf{u}}(\mathbf{v}) = K_k(wt(\mathbf{u})).$$

Proof. Let $wt(\mathbf{u}) = t$ and for simplicity of notations let $\mathbf{u} = (u_1, \ldots, u_t, 0, \ldots, 0)$, $u_i \neq 0$. Choose k positions $h_1, h_2, \ldots, h_k$ and let

$$0 < h_1 < h_2 < \cdots < h_j \leq t < h_{j+1} < \cdots < h_k \leq n.$$

Denote by $D_j \subset W_k$ the set of all vectors of weight k whose nonzero coordinates are $h_1, \ldots, h_k$. Obviously there are $\binom{t}{j}\binom{n-t}{k-j}$ choices for D_j. Now let us evaluate the sum

$$\begin{aligned} \sum_{\mathbf{v}\in D_j} \chi_{\mathbf{u}}(\mathbf{v}) &= \sum_{\mathbf{v}\in D_j} \chi_{u_{h_1}}(v_{h_1}) \cdots \chi_{u_{h_j}}(v_{h_j}) \chi_0(v_{h_{j+1}}) \cdots \chi_0(v_{h_k}) \\ &= \left(\sum_{v\in\mathbb{Z}_q^*} \chi_{u_{h_1}}(v) \right) \cdots \left(\sum_{v\in\mathbb{Z}_q^*} \chi_{u_{h_j}}(v) \right) \left(\sum_{v\in\mathbb{Z}_q^*} \chi_0(v) \right) \cdots \left(\sum_{v\in\mathbb{Z}_q^*} \chi_0(v) \right) \end{aligned}$$

Now applying (1.19) we get

$$\sum_{\mathbf{v}\in D_j} \chi_{\mathbf{u}}(\mathbf{v}) = (-1)^j (q-1)^{k-j}$$

Therefore,

$$\sum_{\mathbf{v}\in W_k} \chi_{\mathbf{u}}(\mathbf{v}) = \sum_{j=0}^{k} (-1)^j \binom{t}{j}\binom{n-t}{k-j}(q-1)^{k-j} = K_k(t).$$

□

Lemma 1.4.18. *Let* $\{A_i\}$, $i = 0, 1, \ldots, n$ *be distance distribution of an* $(n, M)_q$ *code* C *over* $\mathbb{Z}_q$. *Then*

$$\sum_{i=0}^{n} A_i K_k(i) \geq 0$$

for any $k = 0, 1, \ldots, n$. *(Hence* $\{B_i\}_{i=0}^n$ *are nonnegative.)*

Proof. For any vector $\mathbf{z} \in \mathbb{Z}_q^n$ we have

$$\begin{aligned}
0 \leq \left|\sum_{\mathbf{x}\in C} \chi_{\mathbf{x}}(\mathbf{z})\right|^2 &= \left(\sum_{\mathbf{x}\in C} \chi_{\mathbf{x}}(\mathbf{z})\right)\left(\sum_{\mathbf{x}\in C} \overline{\chi_{\mathbf{x}}(\mathbf{z})}\right) \\
&= \left(\sum_{\mathbf{x}\in C} \chi_{\mathbf{x}}(\mathbf{z})\right)\left(\sum_{\mathbf{y}\in C} \chi_{-\mathbf{y}}(\mathbf{z})\right) \\
&= \sum_{(\mathbf{x},\mathbf{y})\in C^2} \chi_{\mathbf{x}}(\mathbf{z})\chi_{-\mathbf{y}}(\mathbf{z}) \\
&= \sum_{(\mathbf{x},\mathbf{y})\in C^2} \chi_{\mathbf{x}-\mathbf{y}}(\mathbf{z}) \\
&= \sum_{i=0}^{n} \sum_{\substack{(\mathbf{x},\mathbf{y})\in C^2 \\ wt(\mathbf{x}-\mathbf{y})=i}} \chi_{\mathbf{x}-\mathbf{y}}(\mathbf{z})
\end{aligned}$$

Summarizing on $\mathbf{z}$ with $wt(\mathbf{z}) = k$ we obtain

$$\begin{aligned} 0 \leq \sum_{\mathbf{z}\in W_k} \left| \sum_{\mathbf{x}\in C} \chi_{\mathbf{x}}(\mathbf{z}) \right|^2 &= \sum_{i=0}^{n} \sum_{\substack{(\mathbf{x},\mathbf{y})\in C^2 \\ wt(\mathbf{x}-\mathbf{y})=i}} \sum_{\mathbf{z}\in W_k} \chi_{\mathbf{x}-\mathbf{y}}(\mathbf{z}) \\ &= \sum_{i=0}^{n} M A_i K_k(i) \\ &= M \sum_{i=0}^{n} A_i K_k(i). \end{aligned}$$

□

The following theorem gives a necessary condition for an orthogonal array.

Lemma 1.4.19. *An $(n, M)_q$ code C over $\mathbb{Z}_q$ is an $OA(M, n, q, t)$ then*

$$\sum_{\mathbf{v}\in C} \chi_{\mathbf{u}}(\mathbf{v}) = 0,$$

for any $\mathbf{u} \in \mathbb{Z}_q^n$ of weight $1 \leq wt(\mathbf{u}) \leq t$.

Proof. If C is $OA(M, n, q, t)$ and $\mathbf{u} \in \mathbb{Z}_q^n$ of weight $wt(\mathbf{u}) = t$, then $\sum_{\mathbf{v}\in C} \chi_{\mathbf{u}}(\mathbf{v})$ is M/q^t times the sum $\sum_{\mathbf{v}\in\mathbb{Z}_q^t} \chi_{\mathbf{u}}(\mathbf{v}) = 0$ by Proposition 1.4.16. □

1.5 Distance distributions of codes and orthogonal arrays

Definition 1.5.1. *Let C be an $OA(M, n, q, t)$ (or a subset of $\mathcal{A}^n$) and $\mathbf{x} \in \mathcal{A}^n$ be a fixed vector. The set of integers $\mathbf{p}(\mathbf{x}) = (p_0, p_1, \ldots, p_n)$ defined by*

$$p_i = |\{\mathbf{u} \in C \mid d(\mathbf{x}, \mathbf{u}) = i\}|$$

*is called the **distance distribution of C with respect to $\mathbf{x}$**.*

Lemma 1.5.2 (Delsart[14, 13])**.** *Let C be $OA(M, n, q, t)$ and $\mathbf{x} \in \mathcal{A}^n(\mathbb{F}_q^n)$. If $\mathbf{p}(\mathbf{x}) = (p_0, p_1, \ldots, p_n)$ is the distance distribution of C with respect to $\mathbf{x}$ then*

$$\sum_{i=0}^{n} p_i K_k(i) = 0 \qquad \text{for } k = 1, \ldots, t. \tag{1.20}$$

Proof. According to Lemma 1.4.17

$$p_i K_k(i) = \sum_{\substack{\mathbf{u}\in C \\ d(\mathbf{x},\mathbf{u})=i}} \sum_{\mathbf{v}\in W_k} \chi_{\mathbf{u}-\mathbf{x}}(\mathbf{v}) = \sum_{\mathbf{v}\in W_k} \left(\chi_{-\mathbf{x}}(\mathbf{v}) \sum_{\substack{\mathbf{u}\in C \\ d(\mathbf{x},\mathbf{u})=i}} \chi_{\mathbf{u}}(\mathbf{v}) \right).$$

Summarizing on $i = 0, 1, \ldots, n$ we have

$$\sum_{i=0}^{n} p_i K_k(i) = \sum_{\mathbf{v}\in W_k} \left(\chi_{-\mathbf{x}}(\mathbf{v}) \sum_{i=0}^{n} \sum_{\substack{\mathbf{u}\in C \\ d(\mathbf{x},\mathbf{u})=i}} \chi_{\mathbf{u}}(\mathbf{v}) \right) = \sum_{\mathbf{v}\in W_k} \left(\chi_{-\mathbf{x}}(\mathbf{v}) \sum_{\mathbf{u}\in C} \chi_{\mathbf{u}}(\mathbf{v}) \right)$$

But according to Lemma 1.4.19

$$\sum_{\mathbf{u}\in C} \chi_{\mathbf{u}}(\mathbf{v}) = \sum_{\mathbf{u}\in C} \chi_{\mathbf{v}}(\mathbf{u}) = 0,$$

for $1 \le wt(\mathbf{v}) \le t$. Hence $\sum_{i=0}^{n} p_i K_k(i) = 0$, for $1 \le k \le t$. □

Theorem 1.5.3. *Let C be $OA(M, n, q, t)$ and $\mathbf{v} \in \mathbb{F}_q^n$. If $\mathbf{p}(\mathbf{v}) = (p_0, p_1, \ldots, p_n)$ is the distance distribution of C with respect to $\mathbf{v}$ then for any polynomial $f(x)$ of degree $\deg f \le t$ the following hold*

(a)

$$\sum_{i=0}^{n} p_i f(i) = f_0 M, \qquad f_0 = \frac{1}{q^n} \sum_{i=0}^{n} f(i) K_i(0) = \frac{1}{q^n} \sum_{i=0}^{n} \binom{n}{i} (q-1)^i f(i) \tag{1.21}$$

where $f(x) = f_0 + \sum_{j=1}^{t} f_j K_j(x)$.

(b)

$$\sum_{i=0}^{n} p_i f(t_i) = a_0 M, \qquad a_0 = \frac{1}{q^n} \sum_{i=0}^{n} \binom{n}{i} (q-1)^i f(t_i) = \frac{1}{q^n} \sum_{i=0}^{n} K_i(0) f(t_i) \tag{1.22}$$

where $f(x) = a_0 + \sum_{j=1}^{t} a_j Q_j(x)$ and $t_i = 1 - \frac{2i}{n}$.

Proof. The values of f_0 and a_0 are given by Theorem 1.4.5 and Theorem 1.4.12.

a) We do the substitution $x = i$ and multiplying by p_i. Then we get

$$p_i f(i) = f_0 p_i + \sum_{j=1}^{t} f_j p_i K_j(i), \quad \text{for } i = 0, 1, \ldots, n.$$

Summarizing on i and we get

$$\sum_{i=0}^{n} p_i f(i) = f_0 \sum_{i=0}^{n} p_i + \sum_{j=1}^{t} \left(f_j \sum_{i=0}^{n} p_i K_j(i) \right) = a_0 M.$$

This follows from Lemma 1.5.2, because C has strength t and

$$\sum_{i=0}^{n} p_i K_j(i) = 0, \quad \text{for } j = 1, \ldots, t.$$

b) Substituting $x = t_i = 1 - \frac{2i}{n}$ and multiplying by p_i we get

$$p_i f(t_i) = a_0 p_i + \sum_{j=1}^{t} a_j p_i Q_j(t_i), \quad \text{for } i = 0, 1, \ldots, n.$$

Summarizing on i we obtain

$$\begin{aligned} \sum_{i=0}^{n} p_i f(t_i) &= a_0 \sum_{i=0}^{n} p_i + \sum_{j=1}^{t} \left(a_j \sum_{i=0}^{n} p_i Q_j(t_i) \right) \\ &= a_0 M + \sum_{j=1}^{t} \left(\frac{a_j}{\binom{n}{j}(q-1)^j} \sum_{i=0}^{n} p_i K_j(i) \right) \end{aligned}$$

Since C has strength t then according to Lemma 1.5.2

$$\sum_{i=0}^{n} p_i K_j(i) = 0, \quad \text{for } j = 1, \ldots, t.$$

Hence

$$\sum_{i=0}^{n} p_i f(t_i) = a_0 M.$$

□

Chapter 2

Computing effectively distance distributions

The knowledge of possible distributions of an orthogonal array with respect to any point is important for solving existence and classification problems. It also gives an useful information about the covering radius of the orthogonal array considered as a q-ary code.

Now we sketch how one can apply the knowledge of possible distance distributions to studying orthogonal arrays and can deduce information about its structure.

In this chapter are used polynomial and combinatorial techniques [13, 23, 17] to compute all feasible distance distributions of ternary orthogonal arrays of respectively small lengths and strengths. We propose a method for computing and reducing of the possibilities of distance distributions of given orthogonal arrays. We use properties of orthogonal arrays (with given parameters) and some relations with their derived orthogonal arrays to reduce the possible distance distributions.

If after applying all constrains there is no distance distributions, the ternary orthogonal arrays with the given parameters does not exist. We improve the know methods [7, 8, 2] for computing and reducing the possibilities for distance distributions of orthogonal arrays.

This is the key for investigating the structure of orthogonal arrays. Then applying the new conditions so that orthogonal arrays must satisfied. If no then we get nonexistence result, i.e there is no $OA(108, 16, 3, 3)$ and confirm the nonexistence result for $OA(108, 17, 3, 3)$.

2.1 Systems, satisfied by feasible distance distributions

Let C be an $OA(M,n,q,t)$ and $\mathbf{x} \in \mathcal{A}^n$ be a fixed vector. The set of integers $\mathbf{p}(\mathbf{x}) = (p_0, p_1, \ldots, p_n)$ defined by

$$p_i = |\{\mathbf{u} \in C \mid \mathrm{d}(\mathbf{x},\mathbf{u}) = i\}|$$

is called the **distance distribution of C with respect to $\mathbf{x}$** (as already defined in1.5.1).

Boyvalenkov and co-authors ([7, 8, 3]) point out that in the general case all feasible distance distributions can be computed as nonnegative integer solutions of certain system of linear equations with Vandermone matrix (t_j^i), where $t_j = 1 - \frac{2j}{n}, j = 0, \ldots, n$, namely

Theorem 2.1.1. *([13, 7]) Let $C \subset H(n,q)$ is an $OA(M,n,q,t)$ and $c \in H(n,q)$ is a fixed point. If $c \in C$, for the distance distribution of C with respect of c the following system holds:*

$$\sum_{i=0}^{n} p_i \left(1 - \frac{2i}{n}\right)^k = f_0|C|, \;\; k = 0, 1, \ldots, t, \tag{2.1}$$

where f_0 is the first coefficient in the expansion of the polynomial t^k by the normalized Krawchouk polynomials.

The well known properties in the theorem below are stated by Bose and Bush ([1]) based on combinatorial arguments and can be found also in [17, Lemma 2.7]. Recently these results are proved in another way by Manev [26]. He also showed different representations of this system. The Manev's results are summarized in the Theorem 2.1.2. Some of these systems can facilitate fast computation of distance distributions. In this section we follow the results of [26].

Theorem 2.1.2 ([26])**.** *Let C be an $OA(M,n,q,t)$ and $\mathbf{v} \in \mathcal{A}^n$.*
If $\mathbf{p}(\mathbf{v}) = (p_0, p_1, \ldots, p_n)$ is the distance distribution of C with respect to $\mathbf{v}$, then for $m = 0, 1, \ldots, t$ and $s = 1, \ldots, t+1$, $\mathbf{p}(\mathbf{v})$ satisfies the following systems:

(i)

$$\sum_{i=0}^{n} \binom{n-i}{m} p_i = \frac{M}{q^m}\binom{n}{m} = \lambda q^{t-m}\binom{n}{m}; \tag{2.2}$$

(ii)

$$\sum_{i=0}^{n} p_i i^m = \frac{M}{q^n} \sum_{i=0}^{n} \binom{n}{i} i^m (q-1)^i; \tag{2.3}$$

(iii)

$$\sum_{i=0}^{n} p_i (n-i)^m = \frac{M}{q^n} \sum_{i=0}^{n} \binom{n}{i} (n-i)^m (q-1)^i; \tag{2.4}$$

(iv)

$$\sum_{i=0}^{n} \binom{i-s}{m} p_i = \frac{M}{q^n} \sum_{i=0}^{n} \binom{n}{i} \binom{i-s}{m} (q-1)^i. \tag{2.5}$$

Proof. (i) Choosing $f(x) = \binom{n-x}{m}$ for $m = 0, 1, \ldots, t$ in Theorem 1.5.3 we obtain

$$\begin{aligned}
\sum_{i=0}^{n} \binom{n-i}{m} p_i &= \frac{M}{q^n} \sum_{i=0}^{n} \binom{n}{i} \binom{n-i}{m} (q-1)^i \\
&= \frac{M}{q^n} \sum_{i=0}^{n} \binom{n}{m} \binom{n-m}{i} (q-1)^i \\
&= \frac{M}{q^n} \binom{n}{m} \sum_{i=0}^{n} \binom{n-m}{i} (q-1)^i \\
&= \frac{M}{q^n} \binom{n}{m} q^{n-m}.
\end{aligned}$$

(ii) We choose in this case $f(x) = x^m \quad for \quad m = 0, 1, \cdots, t$ in Theorem 1.5.3 we obtain (2.3).

(iii) Choose $f(x) = (n-x)^m$ and we obtain (2.4).

(iv) It's nesessary to choose $f(x) = \binom{x-s}{m}$in Theorem 1.5.3 for $m = 0, 1, \cdots, t$ and s is an integer and in this way we obtain the desired identity.

□

These systems (2.2, 2.3, 2.4, 2.5) show that $(p_0, p_1, ..., p_n)$ is a solution of equavalent linear systems with nonnegative integer coefficients. One should find all their nonnegative integer solutions, that is, to select the nonnegative among all integer solutions.

The space of solutions of a linear system $\mathbf{A}\mathbf{x}^\tau = \mathbf{b}$ is the coset $\mathbf{x}_0 + \mathbf{U}$, where $\mathbf{x}_0$ is a partial solution and $\mathbf{U}$ is the null space of $\mathbf{A}$. The considered matrix $\mathbf{A}$ has rank $\operatorname{rank} \mathbf{A} = t + 1$ therefore $\dim \mathbf{U} = n + 1 - (t + 1) = n - t$. Hence $\mathbf{U}$ is generated by the rows of $(n-t) \times (n+1)$ matrix $\mathbf{A}^\perp$ with rank $(n-t)$ that satisfies $\mathbf{A}(\mathbf{A}^\perp)^\tau = \mathbf{O}$.

Therefore any solution of the systems of Theorem 2.1.2 is a sum of a partial solution and a linear combination of the rows of the matrix form by vectors given in Theorem 2.1.4. Instead of this matrix we can use its "systematic" form: all exepting $(t+1)$ fixed columns have only one 1 and zeros in the others positions. Then the $(n-t)$ free variable can be chosen nonnegative and no greater than the upper bound. Distance distribution is any vector with nonnegative values in the fixed $(t+1)$ positions. Due to the special form of the matrix generating the null space formulas for the values in the chosen $(t+1)$ columns can be given. We show this fact by the following example.

The explicit form for $\mathbf{A}^{\perp}$ is given by Theorem 2.1.4 bellow (see [26]). Its proof is based on the following lemma.

Lemma 2.1.3. *([26]) For any $k = 0, 1, 2, \ldots, n$ and s nonnegative integer*

$$\sum_{i=0}^{n} \binom{n}{i} (i+s)^k x^{i+s} = (1+x)^{n-k} g_k(x), \qquad \deg g_k(x) = k+s \tag{2.6}$$

and the leading coefficient of $g_k(x)$ is $(n+s)^k$.

Proof. The proof of the lemma is based on mathematical induction. The Newton binomial gives

$$\sum_{i=0}^{n} \binom{n}{i} x^{i+s} = x^s (1+x)^n.$$

Differentiating and multiplying by x we get

$$\begin{aligned} \sum_{i=0}^{n} \binom{n}{i} (i+s) x^{i+s} &= (1+x)^{n-1} x^s \big[(n+s)x + s\big] \\ &= (1+x)^{n-1} g_1(x), \end{aligned}$$

where $\deg g_1(x) = s+1$ and its leading coefficient is $(n+s)$.

Now we have a base for induction. Assume that (2.6) is true. We prove it for $k+1$. Differentiating and multiplying by x we get

$$\begin{aligned} \sum_{i=0}^{n} \binom{n}{i} (i+s)^{k+1} x^{i+s} &= x\Big[(n-k)(1+x)^{n-k-1} g_k(x) + (1+x)^{n-k} g_k'(x)\Big] \\ &= (1+x)^{n-k-1} x\Big[(n-k) g_k(x) + (1+x) g_k'(x)\Big] \\ &= (1+x)^{n-k-1} g_{k+1}(x), \end{aligned}$$

It is easy to check that the leading coefficient of $g_{k+1}(x)$ is

$$(n-k)(n+s)^k + (k+s)(n+s)^k = (n+s)^{k+1}$$

and

$$\deg g_{k+1} = k+s+1.$$

□

Theorem 2.1.4. *([26]) Let* $\mathbf{A} = (a_{ij}) = (j^i),\ i = 0, 1, \ldots, t,\ j = 1, 2, \ldots, n$. *For* $t < m \leq n$ *the vector*

$$\left(1,\ -\binom{m}{1},\ \binom{m}{2}, \ldots, (-1)^j\binom{m}{j}, \ldots, (-1)^m,\ 0, \ldots, 0\right)$$

and all $n-m-1$ *its cyclic right shifts are linear independent and belong to the null-space of* $\mathbf{A}$. *In partial for* $m = t+1$ *they form a basis of the null-space.*

Proof. Setting $x = -1$ and $n = m$ in (2.6) we obtain

$$\sum_{i=0}^{m}(-1)^{i+s}\binom{m}{i}(i+s)^k = 0,$$

where $k = 0, 1, \ldots, m-1$ and $s = 0, \ldots, n-m$. This proves the theorem. □

We shell need some combinatorical results in order to use them to obtain 'systematic" form in the matrix.

Corollary 2.1.5. *([33, §1.2]) The following identities hold*

(a) $\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m} = \binom{n}{k-m}\binom{n-k+m}{m}$

(b) $\binom{n}{k}\binom{n-k}{m} = \binom{n}{m}\binom{n-m}{k} = \binom{n}{k+m}\binom{k+m}{k}$

Lemma 2.1.6. *([33]) The following hold:*

(a) $S = \sum_{j=0}^{t}(-1)^j\binom{j}{m}\binom{d}{j} = (-1)^m\binom{d}{m}\binom{t-d}{t-m}$;

(b) $S = \begin{cases} (-1)^t\dfrac{d}{d-m}\binom{t}{m}\binom{d-1}{t}, & d \neq m \\ (-1)^m, & d = m \end{cases}$;

$$(c)\quad S=\begin{cases}(-1)^t\dfrac{d-t}{d-m}\binom{t}{m}\binom{d}{t}, & d\neq m\\ (-1)^m, & d=m\end{cases}.$$

Proof. Let us first observe that

$$\begin{aligned}\sum_{j=0}^{t}(-1)^j\binom{d}{j} &= (-1)^0\binom{d}{0}+\sum_{j=1}^{t}(-1)^j\left(\binom{d-1}{j}+\binom{d-1}{j-1}\right)\\ &= 1+\sum_{j=1}^{t}(-1)^j\binom{d-1}{j}+\sum_{j=1}^{t}(-1)^j\binom{d-1}{j-1}\\ &= (-1)^t\binom{d-1}{t}=(-1)^t\frac{d-t}{d}\binom{d}{t}\end{aligned}$$

and using $\binom{j}{m}\binom{d}{j}=\binom{d}{m}\binom{d-m}{j-m}$ and $\binom{n+m-1}{m}=(-1)^m\binom{-n}{m}$.

Now, we are ready to show (a), that is

$$\begin{aligned}S=\sum_{j=0}^{t}(-1)^j\binom{j}{m}\binom{d}{j} &= \sum_{j=0}^{t}(-1)^j\binom{d}{m}\binom{d-m}{j-m}\\ &= \binom{d}{m}\sum_{j=0}^{t}(-1)^j\binom{d-m}{j-m}\\ &= \binom{d}{m}\sum_{k=0}^{t-m}(-1)^{m+k}\binom{d-m}{k}\\ &= (-1)^m\binom{d}{m}\sum_{k=0}^{t-m}(-1)^k\binom{d-m}{k}\\ &= (-1)^m\binom{d}{m}(-1)^{t-m}\binom{d-m-1}{t-m}\\ &= (-1)^m\binom{d}{m}\binom{t-d}{t-m}.\end{aligned}$$

By analogy, we prove identities (b) and (c). □

Lemma 2.1.7. *Let* $\mathbf{R}_t=(r_{ij})=\left(\binom{j}{i}\right)$ *where* $i,j=0,1,2,\ldots,t$. *Its inverse matrix is*

$$\mathbf{R}_t^{-1}=\left((-1)^{i+j}\binom{j}{i}\right).$$

Proof. Using Lemma 2.1.6 (a) we have

$$\sum_{j=0}^{n} r_{kj}(-1)^{j+m} r_{jm} = (-1)^m \sum_{j=0}^{n} (-1)^j \binom{j}{k}\binom{m}{j}$$
$$= (-1)^m (-1)^k \delta_{mk} = \delta_{mk}.$$

□

Upper bounds for $\mathbf{p} = (p_0, p_1, \ldots, p_n)$**.** The trivial upper bound is

$$p_i \leq M$$

but the number $(M+1)^{n-t}$ is too large number even for small parameters M, n, q, t. This makes the computing $\mathbf{p}$ practically infeasible. It turns out that only few p_i can take values close to M. For the most of i the interval for p_i is shorter. Theorem 1.5.3 gives that if $f(i) \geq 0$ for all $i = 0, 1, \ldots, n$ then

$$p_i \leq \frac{f_0 M}{f(i)}.$$

For example we can use (2.1.2)(ii) and (2.1.2)(iii) to obtain an upper bounds for p_i. Each of the linear systems (2.1.2)(ii) and (2.1.2)(iii) gives improvement only for the right or left end of $\mathbf{p}$ but combining both results (as well as with the results from other similar linear systems) we can obtain a significant improvement.

Using different polynomials $f(x)$ we obtain many equivalent linear systems for the distance distribution of the studied orthogonal array. For example

$$f(x) = (2x - n)^k,\ f(x) = (3x - n)^k,\ f(x) = (3n - 4x)^k,\ f(x) = (3x - 2n)^k$$

corresponds to systems with matrices $\mathbf{A} = (a_{ki})$:

$$a_{ki} = (2i - n)^k, \quad a_{ki} = (3i - n)^k, \quad a_{ki} = (3n - 4i)^k, \quad a_{ki} = (3i - 2n)^k$$

2.2 Algorithm

This is an alogorithm for determining possible vectors $\mathbf{p}$.

ALGORITHM

P1. Find the best possible upper bound vector $\mathbf{u}$ for the vectors $\mathbf{p}$.

P2. Set up s. Let s be the number of position before chosen $t+1$ consecutive positions where $\mathbf{u}$ have maximal values. Compute a partial solution from Theorem 2.1.2 (iv) putting zeros in all positions but in the chosen $t+1$ positions.

P3. Apply the **Null Space Algorithm**.
Based on the Theorem2.1.2(iv) we can formule an algorithm for determining the null space.

NS 1. Construct the matrix $\mathbf{A} = (a_{ij}) = \left(\binom{j-s}{i}\right)$. It contains the matrix $\mathbf{R}_t$ defined in Lemma 2.1.7 in columns $s+1, \ldots, s+t+1$.

NS 2. Transform $\mathbf{A}$ into a row echelon form $\mathbf{B}$ by multiplying with $\mathbf{R}_t^{-1}$ (see Lemma 2.1.7) and obtain:

$$\mathbf{B} = \mathbf{R}_t^{-1}\mathbf{A} = (\mathbf{U}_1\, \mathbf{I}_{t+1}\, \mathbf{U}_2),$$

where identity $(t+1) \times (t+1)$ matrix $\mathbf{I}_{t+1}$ in columns $s+1, \ldots, s+t+1$. The matrices $\mathbf{U}_1$ and $\mathbf{U}_2$ are $(t+1) \times s$ and $(t+1) \times (n-t-s)$ matrices respectively.

NS 3. Construct the matrix generating the null space, namely

$$\mathbf{A}^{\perp} = \begin{pmatrix} \mathbf{I}_s & -\mathbf{U}_1^{\tau} & \mathbf{O}_1 \\ \mathbf{O}_2 & -\mathbf{U}_2^{\tau} & \mathbf{I}_{n-t-s} \end{pmatrix},$$

where $\mathbf{O}_1$ and $\mathbf{O}_2$ are zero matrices with suitable size.

NS 4. Generate all linear combinations of the rows of $\mathbf{A}^{\perp}$ with nonnegative coefficients bounded by $\mathbf{u}$.

P4. By adding the partial solution to any vector of the null space find the integer solutions of Theorem 2.1.2 (iv).

P5. Select the solutions that have nonnegative values in $s+1, \ldots, s+t+1$ positions.

Remark Minimization of the upper bound $\mathbf{u}$ is very important. Decreasing even with 1 in one position of $\mathbf{u}$ leads to significant decreasing of numbers of checks. An useful step in this direction is to compute the matrix generating the null space (i.e. NS 3) for $s = n-t$ or $n-t-1$ and compare its entries with the corresponding partial solution.

Solutions with zero first coordinate are distance distribution with respect to an external point for the orthogonal array while ones with nonzero first coordinate close to M. For the most of i the interval for p_i is quit shorter. Indeed, using again correspond to distributions with respect to internal point. If the first coordinate is greater then 1 it means that the point appears more then one time, i.e., the orthogonal array is a multi-set.

Example 2.2.1. *Let us consider* $OA(M = 6 \cdot 3^5 = 1458, n = 13, q = 3, t = 5)$ *and the parameter* $s = 9$. *The matrix* $\mathbf{A}$ *and the column* $\mathbf{b}$ *of free terms given*

by Theorem 2.1.2 (i)

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 13 & 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 78 & 66 & 55 & 45 & 36 & 28 & 21 & 15 & 10 & 6 & 3 & 1 & 0 & 0 \\ 286 & 220 & 165 & 120 & 84 & 56 & 35 & 20 & 10 & 4 & 1 & 0 & 0 & 0 \\ 715 & 495 & 330 & 210 & 126 & 70 & 35 & 15 & 5 & 1 & 0 & 0 & 0 & 0 \\ 1287 & 792 & 462 & 252 & 126 & 56 & 21 & 6 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1458 \\ 6318 \\ 12636 \\ 15444 \\ 12870 \\ 7722 \end{pmatrix}$$

by Theorem 2.1.2 (ii)

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 0 & 1 & 4 & 9 & 16 & 25 & 36 & 49 & 64 & 81 & 100 & 121 & 144 & 169 \\ 0 & 1 & 8 & 27 & 64 & 125 & 216 & 343 & 512 & 729 & 1000 & 1331 & 1728 & 2197 \\ 0 & 1 & 16 & 81 & 256 & 625 & 1296 & 2401 & 4096 & 6561 & 10000 & 14641 & 20736 & 28561 \\ 0 & 1 & 32 & 243 & 1024 & 3125 & 7776 & 16807 & 32768 & 59049 & 100000 & 161051 & 248832 & 371293 \end{pmatrix}, \begin{pmatrix} 1458 \\ 12636 \\ 113724 \\ 1057212 \\ 10110204 \\ 99135036 \end{pmatrix}$$

by Theorem 2.1.2 (iii)

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 13 & 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 169 & 144 & 121 & 100 & 81 & 64 & 49 & 36 & 25 & 16 & 9 & 4 & 1 & 0 \\ 2197 & 1728 & 1331 & 1000 & 729 & 512 & 343 & 216 & 125 & 64 & 27 & 8 & 1 & 0 \\ 28561 & 20736 & 14641 & 10000 & 6561 & 4096 & 2401 & 1296 & 625 & 256 & 81 & 16 & 1 & 0 \\ 371293 & 248832 & 161051 & 100000 & 59049 & 32768 & 16807 & 7776 & 3125 & 1024 & 243 & 32 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1458 \\ 6318 \\ 31590 \\ 174798 \\ 1048086 \\ 6717438 \end{pmatrix}$$

by Theorem 2.1.2 (iv)

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -7 & -6 & -5 & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 28 & 21 & 15 & 10 & 6 & 3 & 1 & 0 & 0 & 1 & 3 & 6 & 10 & 15 \\ -84 & -56 & -35 & -20 & -10 & -4 & -1 & 0 & 0 & 0 & 1 & 4 & 10 & 20 \\ 210 & 126 & 70 & 35 & 15 & 5 & 1 & 0 & 0 & 0 & 0 & 1 & 5 & 15 \\ -462 & -252 & -126 & -56 & -21 & -6 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 6 \end{pmatrix}, \begin{pmatrix} 1458 \\ 2430 \\ 2916 \\ 1080 \\ 1044 \\ -612 \end{pmatrix}.$$

We obatin the matrix $B = R^{-1}A$ we need the matrix R^{-1}, i.e.

$$R^{-1} = \begin{pmatrix} 1 & -1 & 1 & -1 & 1 & -1 \\ 0 & 1 & -2 & 3 & -4 & 5 \\ 0 & 0 & 1 & -3 & 6 & -10 \\ 0 & 0 & 0 & 1 & -4 & 10 \\ 0 & 0 & 0 & 0 & 1 & -5 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

We get the matrix B

$$B = \begin{pmatrix} 792 & 462 & 252 & 126 & 56 & 21 & 6 & 1 & 0 & 0 & 0 & 0 & 0 & -1 \\ -3465 & -1980 & -1050 & -504 & -210 & -70 & -15 & 0 & 1 & 0 & 0 & 0 & 0 & 6 \\ 6160 & 3465 & 1800 & 840 & 336 & 105 & 20 & 0 & 0 & 1 & 0 & 0 & 0 & -15 \\ -5544 & -3080 & -1575 & -720 & -280 & -84 & -15 & 0 & 0 & 0 & 1 & 0 & 0 & 20 \\ 2520 & 1386 & 700 & 315 & 120 & 35 & 6 & 0 & 0 & 0 & 0 & 1 & 0 & -15 \\ -462 & -252 & -126 & -56 & -21 & -6 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 6 \end{pmatrix}$$

and the matrix $B^{\perp}$

$$B^{\perp} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 7 & -28 & 84 & -210 & 462 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 6 & -21 & 56 & -126 & 252 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 5 & -15 & 35 & -70 & 126 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 4 & -10 & 20 & -35 & 56 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 3 & -6 & 10 & -15 & 21 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 2 & -3 & 4 & -5 & 6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -6 & -15 & -20 & -15 & -6 & 1 \end{pmatrix}$$

The obvious number of potential solutions of (2.1.2)(ii) (and any equivalent to it linear system) is $(M+1)^{n+1}$. *For the given above example of* $OA(M = 6 \cdot 3^5 = 1458, n = 13, q = 3, t = 5)$ *this number is* $1459^{14} \approx 19 * 10^{43}$, *which is enormous. The obtained upper bound reduce it to* $\approx 10^{31}$, *but this number is still large for a direct check by replacing in the system. Hence we choose another approach. In the case of* $OA(M = 6 \cdot 3^5 = 1458, n = 13, q = 3, t = 5)$ *we can obtain*

$$\mathbf{p} \leq \mathbf{u} = (6, 9, 16, 30, 61, 137, 367, 772, 1263, 1404, 991, 615, 398, 266).$$

2.3 Our approach

Let us consider the system (iv) in Theorem 2.1.2 in details.

$$A_s p^{\tau} = a, \tag{2.7}$$

where

$$A_s = (a_{kl}) = \left(\binom{l-s}{k} \right)$$

is a $(t+1) \times (n+1)$ matrix. The vector $a = (a_0, a_1, \ldots, a_t)^{\tau}$ is determined by

$$a_k = \frac{M}{q^n} \sum_{i=0}^{n} \binom{n}{i} \binom{i-s}{k} (q-1)^i,$$

where $k = 0, \ldots, t$. Columns of A corresponding to $l = s, \ldots, s+t$ form $(t+1)\times(t+1)$ matrix $R_t = (r_{ij}) = (\binom{j}{i})$. Multiplying the system (3.1) with R_t^{-1} we get $Bp^{\tau} = b$,

where $B = R_t^{-1}A = (b_{ml})$ and $b = (b_0, \ldots, b_t)^\tau$, that is,

$$b_{ml} = (-1)^m \sum_{j=0}^{t} (-1)^j \binom{j}{m} \binom{l-s}{j}, \quad m = 0, 1, \ldots, t,\ l = 0, 1, \ldots, n$$

and

$$b_m = (-1)^m \lambda q^{t-n} \sum_{i=0}^{n} \left(\binom{n}{i} (q-1)^i \sum_{j=0}^{t} \binom{j}{m} \binom{i-s}{j} \right), \quad m = 0, 1, \ldots, t. \quad (2.8)$$

Based on Lemma 2.1.6 we can evaluate the elements of the matrix B by the next theorem.

Theorem 2.3.1. *The following hold:*

(a) $b_{ml} = (-1)^{2m} \binom{l-s}{m} \binom{t-l+s}{t-m} = \binom{l-s}{m} \binom{t-l+s}{t-m}$;

(b) $b_{ml} = \begin{cases} (-1)^{m+t} \dfrac{l-s-t}{l-s-m} \binom{t}{m} \binom{l-s}{t}, & l \neq s+m \\ 1, & l = s+m \end{cases}$

Therefore $B = (U_1 I_{t+1} U_2)$, where

- $U_1 = (b_{ml})$ is $(t+1) \times s$ matrix $(l = 0, 1, \ldots, s-1)$;
- $U_2 = (b_{ml})$ is $(t+1) \times (n-s-t)$ matrix $(l = s+t+1, \ldots, n)$;
- I_{t+1} is identity $(t+1) \times (t+1)$ matrix, placed in columns $l = s+t+1, \ldots, n$.

Now we can simplify expression for b_m. Applying Lemma 2.1.6 to (2.8) we get

$$b_m = (-1)^m \lambda q^{t-n} \sum_{i=0}^{n} \binom{n}{i} (q-1)^i (-1)^m \binom{i-s}{m} \binom{t+s-i}{t-m}$$

or equivalently

$$b_m = (-1)^{m+t} \lambda q^{t-n} \binom{t}{m} \sum_{i=0}^{n} \binom{n}{i} \binom{i-s}{t} \frac{i-s-t}{i-s-m} (q-1)^i,$$

where $m = 0, 1, \ldots, t$.

The vector $(b_0, b_1, \ldots, b_t)$ is a partial solution, i.e. any solution is a sum of this and vector of the Null space of B, i.e. linear combination of rows of

$$G = \begin{pmatrix} I_s & -U_1^\tau & O_1 \\ O_2 & -U_2^\tau & I_{n-t-s} \end{pmatrix}.$$

Thus the received formula give us possibility to obtain some bounds for b_{ml} and b_m $(l = 0, \ldots, s-1, s+t+1, \ldots, n)$, otherwise b_{ml} is 1 or 0 when $l = s, \ldots, s+t$.

Corollary 2.3.2. *The numbers b_{ml} has the same sign with $(-1)^m$ for t even number and for every $l = 0, 1, \ldots, s-1, s+t+1, \ldots, n$.*

Proof. Let us notice that $\dfrac{l-s-t}{l-s-m} > 0$. This is true because

- if $l \leq s \Rightarrow l - s \leq 0 \Rightarrow \dfrac{l-s-t}{l-s-m} > 0$
- if $l > s+t \Rightarrow l - s \geq t+1 \Rightarrow \dfrac{l-s-t}{l-s-m} > 0$ $(m \leq t)$.

Using Theorem 2.3.1 (b) and facts that in any case $\dfrac{l-s-t}{l-s-m} > 0$ and $\binom{l-s}{t} \geq 0$ whether $l - s$ is greater than or less than 0 for even t. □ □

Corollary 2.3.3. *For t even number the inequality holds*

$$p_l \leq \left\lfloor \frac{b_m}{b_{ml}} \right\rfloor, \text{ for } l = 0, 1, ..s-1, s+t+1, \ldots, n$$

Proof. The numbers b_m has the same sign as b_{ml}. □ □

The situation when t is odd number is a more complicate, because $\binom{l-s}{t} < 0$ for $l = 0, 1, \ldots, s-1$. Therefore for given m the numbers b_{ml} in the matrix U_1 are with one sign, but have the opposite in matrix U_2.

2.4 Relation between distance distributions of OA(M,n,q,t) and related orthogonal array

In what follows we show how we study orthogonal arrays applying the knowledge of possible distance distributions and derive information about its structure.

Let C be an $OA(M, n, q, t)$ and we can assume that C contains the all-zero vector. Let C be the orthogonal array obtained from C by deleting the first column. Denote by C_i, $i = 0, 1, \ldots, q-1$ the set obtained by taking all rows of C with the i-th element of $\mathcal{A}$ in the first column and then deleting the first column. (C_0 corresponds to 0 in the first column.) According to Proposition 1.2.1

$$C \text{ is } OA(M, n-1, q, t) \qquad \text{and} \qquad C_i \text{ is } OA(M/q, n-1, q, t-1).$$

We compute all possible distance distributions of C, C_i, C using described algorithm, and any other necessary arrays derived from C.

Let $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in C$, i.e., $\mathbf{c}_0 = (c_2, \ldots, c_n) \in C_0$ or C_i. The distance distribution of C with respect to $\mathbf{c}$ is $\mathbf{p}(\mathbf{c}) = (p_0, p_1, \ldots, p_n)$ and $\mathbf{p}^0(\mathbf{c}_0) = (p_0^0, p_1^0, \ldots, p_{n-1}^0)$ of C_0 (or C_i) to $\mathbf{c}_0$, respectively.

We say that a vector $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ ***dominate*** another vector $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ if $a_i \geq b_i$ for all $i = 1, \ldots, n$.

Corollary 2.4.1. *If vector $p = (p_0, p_1, \ldots, p_n)$ is a a distance distribution of $OA(M, n, q, t)$ array C then it satisfies the following conditions*

(i) $(p_0, p_1, \ldots, p_{n-1})$ *dominates* $(p_0^0, p_1^0, \ldots, p_{n-1}^0)$, *when* $p_0^0 \geq 1$;

(ii) $(p_1, p_2, \ldots, p_n)$ *dominates* $(p_0^0, p_1^0, \ldots, p_{n-1}^0)$ *when* $p_0^0 = 0$;

(iii) *the difference*

$$\overline{p}(c_0) = (\bar{p}_0, \bar{p}_1, \ldots, \bar{p}_{n-1}) = (p_1 - p_1^0, \ldots, p_{n-1} - p_{n-1}^0, p_n)$$

has to be the distance distribution of $C_1 \cup \cdots \cup C_{q-1}$ with respect to the external point c_0;

(iv) $\overset{\mathrm{v}}{p}(c_0) = \overline{p}(c_0) + p^0(c_0)$ *has to be a distance distribution of* $\overset{\mathrm{v}}{C}$ *with respect to* c_0.

We will called $\mathbf{p}$, $\overline{\mathbf{p}}(\mathbf{c})$, $\mathbf{p}^0$ ***successors*** of $\mathbf{p}$ and $\mathbf{p}$ their ***parent vector***.

When we delete different columns we can obtain not only different C_i but different values for $\mathbf{p}$, $\overline{\mathbf{p}}(\mathbf{c})$, $\mathbf{p}^0$. The following result holds

Theorem 2.4.2 ([7, 26])**.** *Let $\overline{p}^{(1)}, \overline{p}^{(2)}, \ldots, \overline{p}^{(s)}$ be all possible successors of p and let $\overline{p}^{(i)}$ be obtained in k_i cases of deleting of a column, $i = 1, 2, \ldots, s$. Then the integers k_i satisfy*

$$\left| \begin{array}{l} k_1 + k_2 + \cdots + k_s = n \\ k_1\overline{p}^{(1)} + k_2\overline{p}^{(2)} + \cdots + k_s\overline{p}^{(s)} = (p_1, 2p_2, \ldots, np_n) \\ k_i \geq 0 \end{array} \right.$$

Proof. We calculate the nonzero positions of the submatrix of rows at distance i from c (called i-block)in two ways.

Calculating by rows we get the right side ip_i, while the calculation by columns gives the left side of the equation. □

Example 2.4.3. We demonstrate the aforesaid by the same orthogonal array $C = OA(18, 7, 3, 2)$. In this case

$$C = OA(18, 6, 3, 2) \qquad \text{and} \qquad C_i = OA(6, 6, 3, 1)$$

There are 3 possible distance distributions with respect to an internal point for C, namely

$$(1, 0, 0, 2, 9, 6, 0)$$
$$(1, 0, 0, 1, 12, 3, 1)$$
$$(1, 0, 0, 0, 15, 0, 2)$$

For $C_i = OA(6, 6, 3, 1)$ we have 10 possible distribution with respect to internal point and 29 with respect to external point.

Distance distributions
1 0 0 0 1 4 0
1 0 0 0 2 2 1
1 0 0 0 3 0 2
1 0 0 1 0 3 1
1 0 0 1 1 1 2
1 0 0 2 0 0 3
1 0 1 0 0 2 2
1 0 1 0 1 0 3
1 1 0 0 0 1 3
2 0 0 0 0 0 4

Table 2.1: Distance distributions for internal point $OA(6, 6, 3, 1)$

For $\mathbf{c} \in C$ we obtained two possible distributions $\mathbf{p}(\mathbf{c}) = (1, 0, 0, 1, 0, 15, 1, 0)$ and $\mathbf{p}(\mathbf{c}) = (1, 0, 0, 0, 3, 12, 2, 0)$. The first distribution dominates one while the second dominates three possible distributions for C_0. The same is situation with C_1 and C_2, namely

Hence only 4 among 10 distribution of C_0 with respect to inner point and only 3 among 29 distributions of C_i with respect to external point are indeed possible. The last column of the table gives the distribution $\overline{\mathbf{p}}$ of $C_1 \cup C_2$ with respect to the external point $\mathbf{c}_0$. One can check that for all rows the condition (iv) of Proposition 2.4.1 holds.

Since we can assume $\mathbf{c} = \mathbf{0}$ the presented distribution can be considered as weight distributions of C_i and $C_1 \cup \cdots \cup C_{q-1}$. Therefore we obtain information about weight structure of C. It is presented in Table As usually the vectors in the table present from left to right the number of words with weight from zero to 6.

Distance distributions
0 0 0 0 6 0 0
0 0 0 1 4 1 0
0 0 0 2 2 2 0
0 0 0 2 3 0 1
0 0 0 3 0 3 0
0 0 0 3 1 1 1
0 0 0 4 0 0 2
0 0 1 0 3 2 0
0 0 1 0 4 0 1
0 0 1 1 1 3 0
0 0 1 1 2 1 1
0 0 1 2 0 2 1
0 0 1 2 1 0 2
0 0 2 0 0 4 0
0 0 2 0 1 2 1
0 0 2 0 2 0 2
0 0 2 1 0 1 2
0 0 3 0 0 0 3
0 1 0 0 2 3 0
0 1 0 0 3 1 1
0 1 0 1 0 4 0
0 1 0 1 1 2 1
0 1 0 1 2 0 2
0 1 0 2 0 1 2
0 1 1 0 0 3 1
0 1 1 0 1 1 2
0 1 1 1 0 0 3
0 2 0 0 0 2 2
0 2 0 0 1 0 3

Table 2.2: Distance distributions for external point $OA(6, 6, 3, 1)$

Let consider the case $\mathbf{p} = (1, 0, 0, 0, 3, 12, 2, 0)$. It has 3 possible successors (see Table 2.4)

$$\begin{aligned} \overline{\mathbf{p}}^{(1)} &= (0, 0, 0, 2, 8, 2, 0) \\ \overline{\mathbf{p}}^{(2)} &= (0, 0, 0, 1, 10, 1, 0) \\ \overline{\mathbf{p}}^{(3)} &= (0, 0, 0, 0, 12, 0, 0) \end{aligned}$$

Distance distributions	for external point $OA(18,7,3,2)$
0 0 0 0 14 0 0 4	0 0 1 2 4 8 1 2
0 0 0 1 12 0 2 3	0 0 1 3 3 5 6 0
0 0 1 3 1 11 0 2	0 0 1 3 2 8 3 1
0 0 0 2 10 0 4 2	0 0 1 4 0 8 5 0
0 0 0 2 9 3 1 3	0 0 2 0 6 4 6 0
0 0 0 3 8 0 6 1	0 0 2 0 5 7 3 1
0 0 0 3 7 3 3 2	0 0 2 0 4 10 0 2
0 0 0 3 6 6 0 3	0 0 2 1 3 7 5 0
0 0 0 4 6 0 8 0	0 0 2 1 2 10 2 1
0 0 0 4 5 3 5 1	0 0 2 2 0 10 4 0
0 0 0 4 4 6 2 2	0 0 3 0 0 12 3 0
0 0 0 5 3 3 7 0	0 1 0 0 8 3 6 0
0 0 0 5 2 6 4 1	0 1 0 0 7 6 3 1
0 0 0 5 1 9 1 2	0 1 0 0 6 9 0 2
0 0 0 6 0 6 6 0	0 1 0 1 5 6 5 0
0 0 1 0 10 2 3 2	0 1 0 1 4 9 2 1
0 0 1 0 9 5 0 3	0 1 0 2 2 9 4 0
0 0 1 1 8 2 5 1	0 1 0 2 1 12 1 1
0 0 1 1 7 5 2 2	0 1 1 0 2 11 3 0
0 0 1 2 6 2 7 0	0 1 1 0 1 14 0 1
0 0 1 2 5 5 4 1	

Table 2.3: Distance distributions for external point $OA(18,7,3,2)$

C	C_0	C_1 or C_2	$\overline{\mathbf{p}}$
1, 0, 0, 1, 0, 15, 1, 0	1, 0, 0, 1, 0, 3, 1	0, 0, 0, 0, 6, 0, 0	0, 0, 0, 0, 12, 0, 0
1, 0, 0, 0, 3, 12, 2, 0	1, 0, 0, 0, 1, 4, 0	0, 0, 0, 0, 6, 0, 0	0, 0, 0, 2, 8, 2, 0
	1, 0, 0, 0, 2, 2, 1	0, 0, 0, 1, 4, 1, 0	0, 0, 0, 1, 10, 1, 0
	1, 0, 0, 0, 3, 0, 2	0, 0, 0, 2, 2, 2, 0	0, 0, 0, 0, 12, 0, 0

Table 2.4: Possible distributions and their successors.

Then Theorem 2.4.2 gives

$$
\left|\begin{array}{l}
k_1+k_2+k_3=7 \\
k_1\begin{pmatrix}0\\0\\0\\2\\8\\2\\0\end{pmatrix}+k_2\begin{pmatrix}0\\0\\0\\1\\10\\1\\0\end{pmatrix}+k_3\begin{pmatrix}0\\0\\0\\0\\12\\0\\0\end{pmatrix}=\begin{pmatrix}0\\0\\0\\12\\60\\12\\0\end{pmatrix} \\
k_i\geq 0,\ i=1,2,3
\end{array}\right.
$$

C_0	1,0,0,1,0,3,1	1,0,0,0,1,4,0	1,0,0,0,1,4,0	1,0,0,0,2,2,1	1,0,0,0,3,0,2
C_1	0,0,0,0,6,0,0	0,0,0,0,6,0,0	0,0,0,1,4,1,0	0,0,0,0,6,0,0	0,0,0,0,6,0,0
C_2	0,0,0,0,6,0,0	0,0,0,2,2,2,0	0,0,0,1,4,1,0	0,0,0,1,4,1,0	0,0,0,0,6,0,0

The above system is equivalent to

$$\left|\begin{array}{l} k_1 = 5 + k_3 \\ k_2 = 2 - 2k_3 \\ k_i \geq 0,\ i = 1,2,3 \end{array}\right.$$

The only integer solutions are

$$k_1 = 5,\ k_2 = 2,\ k_3 = 0$$
$$k_1 = 6,\ k_2 = 0,\ k_3 = 1$$

Now let consider the case $\mathbf{p} = (1,0,0,1,0,15,1,0)$. It has only 1 possible successor and gives the system

$$\left|\begin{array}{l} k_1 = 7 \\ k_1 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 12 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 3 \\ 0 \\ 75 \\ 6 \\ 0 \end{pmatrix}, \\ k_i \geq 0,\ i = 1,2,3 \end{array}\right.$$

which has obviously no solution.

Hence we collect much information about the structures of C that can be used for constructing and classification of such orthogonal arrays. Both obtained values for k_i are realized in existing arrays. All nonisomorphic $OA(18,n,3,2)$ for $3 \leq n \leq 7$ are classified in [16] and we refer the interested reader to it for more details.

2.5 Results

2.5.1 Nonexistence results

Theorem 2.5.1. *The minimal index for ternary arrays with strength $t = 3$ and length 17 and 16 is $\lambda = 5$.*

Proof. We have to prove that $OA(108, 17, 3, 3)$ and $OA(108, 16, 3, 3)$ do not exist. Based on the given above algorithms and obtained results we do the following:

1. First we compute all possible distance distributions $\mathbf{p} = (p_0, p_1, \ldots, p_n)$ with respect to internal points for $OA(108, 17, 3, 3)$ and $OA(108, 16, 3, 3)$ are 10 and 49, respectively.

   $OA(108, 17, 3, 3)$ has 10 possible DDs:

$$\{[1,0,0,0,0,0,0,0,0,0,0,8,87,2,0,0,3,1,6],$$
$$[1,0,0,0,0,0,0,0,0,0,0,10,81,7,0,0,1,2,6],$$
$$[1,0,0,0,0,0,0,0,0,0,0,10,83,1,5,0,1,0,7],$$
$$[1,0,0,0,0,0,0,0,0,0,0,11,79,7,1,1,1,0,7],$$
$$[1,0,0,0,0,0,0,0,0,0,1,6,87,3,1,0,1,2,6],$$
$$[1,0,0,0,0,0,0,0,0,0,1,6,88,1,0,4,0,0,7],$$
$$[1,0,0,0,0,0,0,0,0,0,1,7,85,3,2,1,1,0,7],$$
$$[1,0,0,0,0,0,0,0,0,0,3,0,93,1,0,2,1,0,7],$$
$$[1,0,0,0,0,0,0,0,0,1,1,0,94,2,0,0,2,0,7],$$
$$[1,0,0,0,0,0,0,0,0,1,1,2,88,7,0,0,0,1,7]\}$$

   $OA(108, 16, 3, 3)$ has 49 possible DDs:

$$\{[1,0,0,0,0,0,0,0,0,0,72,24,0,0,0,8,3], \quad [1,0,0,0,0,0,0,0,0,0,73,22,0,0,5,2,5],$$
$$[1,0,0,0,0,0,0,0,0,0,74,18,5,0,0,6,4], \quad [1,0,0,0,0,0,0,0,0,0,74,19,2,2,2,3,5],$$
$$[1,0,0,0,0,0,0,0,0,0,75,16,5,0,5,0,6], \quad [1,0,0,0,0,0,0,0,0,0,75,17,1,6,1,1,6],$$
$$[1,0,0,0,0,0,0,0,0,0,76,12,10,0,0,4,5], \quad [1,0,0,0,0,0,0,0,0,0,76,13,7,2,2,1,6],$$
$$[1,0,0,0,0,0,0,0,0,0,78,6,15,0,0,2,6], \quad [1,0,0,0,0,0,0,0,0,0,80,0,20,0,0,0,7],$$
$$[1,0,0,0,0,0,0,0,0,1,70,24,1,1,0,6,4], \quad [1,0,0,0,0,0,0,0,0,1,71,22,1,1,5,0,6],$$
$$[1,0,0,0,0,0,0,0,0,1,72,18,6,1,0,4,5], \quad [1,0,0,0,0,0,0,0,0,1,72,19,3,3,2,1,6],$$
$$[1,0,0,0,0,0,0,0,0,1,74,12,11,1,0,2,6], \quad [1,0,0,0,0,0,0,0,0,1,76,6,16,1,0,0,7],$$

$[1,0,0,0,0,0,0,0,0,0,2,67,27,0,0,3,3,5]$, $[1,0,0,0,0,0,0,0,0,0,2,68,24,2,2,0,4,5]$,
$[1,0,0,0,0,0,0,0,0,0,2,69,21,5,0,3,1,6]$, $[1,0,0,0,0,0,0,0,0,0,2,70,18,7,2,0,2,6]$,
$[1,0,0,0,0,0,0,0,0,0,2,72,12,12,2,0,0,7]$, $[1,0,0,0,0,0,0,0,0,0,3,65,27,1,1,3,1,6]$,
$[1,0,0,0,0,0,0,0,0,0,3,66,24,3,3,0,2,6]$, $[1,0,0,0,0,0,0,0,0,0,3,68,18,8,3,0,0,7]$,
$[1,0,0,0,0,0,0,0,0,0,4,61,32,0,0,1,4,5]$, $[1,0,0,0,0,0,0,0,0,0,4,63,26,5,0,1,2,6]$,
$[1,0,0,0,0,0,0,0,0,0,4,64,24,4,4,0,0,7]$, $[1,0,0,0,0,0,0,0,0,0,4,65,20,10,0,1,0,7]$,
$[1,0,0,0,0,0,0,0,0,0,5,59,32,1,1,1,2,6]$, $[1,0,0,0,0,0,0,0,0,0,5,60,30,0,5,0,0,7]$,
$[1,0,0,0,0,0,0,0,0,0,5,61,26,6,1,1,0,7]$, $[1,0,0,0,0,0,0,0,0,0,6,57,32,2,2,1,0,7]$,
$[1,0,0,0,0,0,0,0,0,0,8,50,40,0,0,2,0,7]$, $[1,0,0,0,0,0,0,0,0,0,10,44,45,0,0,0,1,7]$,
$[1,0,0,0,0,0,0,0,0,1,0,67,28,1,0,1,4,5]$, $[1,0,0,0,0,0,0,0,0,1,0,68,26,0,4,0,2,6]$,
$[1,0,0,0,0,0,0,0,0,1,0,69,22,6,0,1,2,6]$, $[1,0,0,0,0,0,0,0,0,1,0,70,20,5,4,0,0,7]$,
$[1,0,0,0,0,0,0,0,0,1,0,71,16,11,0,1,0,7]$, $[1,0,0,0,0,0,0,0,0,1,1,65,28,2,1,1,2,6]$,
$[1,0,0,0,0,0,0,0,0,1,1,66,26,1,5,0,0,7]$, $[1,0,0,0,0,0,0,0,0,1,1,67,22,7,1,1,0,7]$,
$[1,0,0,0,0,0,0,0,0,1,2,63,28,3,2,1,0,7]$, $[1,0,0,0,0,0,0,0,0,1,4,56,36,1,0,2,0,7]$,
$[1,0,0,0,0,0,0,0,0,1,6,50,41,1,0,0,1,7]$, $[1,0,0,0,0,0,0,0,0,2,0,62,32,2,0,2,0,7]$,
$[1,0,0,0,0,0,0,0,0,2,2,56,37,2,0,0,1,7]$, $[1,0,0,0,0,0,0,0,1,0,0,64,30,4,0,0,1,7]$,
$[1,0,0,0,0,0,0,0,1,0,1,60,36,0,1,0,1,7]$ }

2. The same distributions $\mathbf{p}^0 = (p_0^0, p_1^0, \ldots, p_{n-1}^0)$ for residual arrays $OA(36,16,3,2)$ and $OA(36,15,3,2)$ are 6 and 12, respectively.
(15, 36, 2) has 12 possible DDs:

$\{[1,0,0,0,0,0,0,0,0,0,29,3,2,1,0,0]$, $[1,0,0,0,0,0,0,0,0,0,30,0,5,0,0,0]$,
$[1,0,0,0,0,0,0,0,0,1,26,6,1,1,0,0]$, $[1,0,0,0,0,0,0,0,0,1,27,3,4,0,0,0]$,
$[1,0,0,0,0,0,0,0,0,2,23,9,0,1,0,0]$, $[1,0,0,0,0,0,0,0,0,2,24,6,3,0,0,0]$,
$[1,0,0,0,0,0,0,0,0,3,21,9,2,0,0,0]$, $[1,0,0,0,0,0,0,0,0,4,18,12,1,0,0,0]$,
$[1,0,0,0,0,0,0,0,0,5,15,15,0,0,0,0]$, $[1,0,0,0,0,0,0,0,1,0,24,8,2,0,0,0]$,
$[1,0,0,0,0,0,0,0,1,1,21,11,1,0,0,0]$, $[1,0,0,0,0,0,0,0,1,2,18,14,0,0,0,0]\}$

(16, 36, 2) has 6 possible DDs:

$$\{[1,0,0,0,0,0,0,0,0,0,5,27,2,1,0,0,0],$$
$$[1,0,0,0,0,0,0,0,0,0,6,24,5,0,0,0,0],$$
$$[1,0,0,0,0,0,0,0,0,0,1,2,30,1,1,0,0,0],$$
$$[1,0,0,0,0,0,0,0,0,0,1,3,27,4,0,0,0,0],$$
$$[1,0,0,0,0,0,0,0,0,0,2,0,30,3,0,0,0,0],$$
$$[1,0,0,0,0,0,0,0,0,1,0,0,32,2,0,0,0,0]\}$$

3. Then we apply Corollary 2.4.1. Only 9 vectors $\mathbf{p}$ of $OA(108,17,3,3)$ dominate internal distributions $\mathbf{p}^0$ of $OA(36,16,3,2)$.

4. For any pair $(\mathbf{p},\mathbf{p}^0)$ we compute the difference $\overline{p}(c) = (\bar{p}_0,\bar{p}_1,\ldots,\bar{p}_{n-1})$ (see Corollary 2.4.1). Then we test whether $\overline{p}(c)$ is an external distribution for $C_1 \cup C_2$ that are $OA(72,16,3,2)$ and $OA(72,15,3,2)$ arrays, respectively. This means that the set of received distance distributions have to satisfy system of equations (Theorem 2.1.2).

5. In the case $n = 17$ test shows that none of $\overline{p}(c)$ satisfies the system. The obtained controduction proves that $OA(108,17,3,3)$ does not exist.

6. The case $n = 16$ is more complicated. For seven of pairs $(\mathbf{p},\mathbf{p}^0)$ the corresponding vectors $\overline{p}(c)$ satisfy the system for $OA(72,15,3,2)$. Hence we have to apply Theorem 2.4.2 for the rest $\overline{p}(c)$. No one passes this test. Therefore $OA(108,16,3,3)$ does not exist.

□

Remark. The result of nonexistence of $OA(108,17,3,3)$ was already obtained by M. Stoyanova and T. Marinova, but we receive it independently using another approach. That's why we wrote a paper together [2].

2.5.2 Structural results

Structure of $OA(108,15,3,3)$ From [2] we have that $OA(108,15,3,3)$ has 119 possible distace ditribution and after applying the aforesaid approach we obtain 4 from 119 possible internal distance distribution for $OA(108,15,3,3)$ which pass all tests.

$$[1,0,0,0,0,0,0,0,15,0,84,0,0,0,0,8]$$

$$[1,0,0,0,0,0,0,1,11,6,80,1,0,0,0,8]$$

$$[1,0,0,0,0,0,0,2,7,12,76,2,0,0,0,8]$$

$$[1,0,0,0,0,0,0,3,3,18,72,3,0,0,0,8].$$

Hence we cannot get contradictions but we have collected much information for the structure of array. It gives us a hope that we succeed in construction $OA(108,15,3,3)$ array.

Structure of $OA(1458,16,3,5)$

In this case we compute only one possible internal distribution:

$$\mathbf{p} = (1,0,0,0,0,0,0,0,270,320,0,0,840,0,0,0,27),$$

which dominates only one inner distribution of C_0, namely

$$\mathbf{p}^0 = (1,0,0,0,0,0,0,0,135,140,0,0,210,0,0,0).$$

Then

$$\overline{\mathbf{p}} = (0,0,0,0,0,0,0,0,135,180,0,0,630,0,0,0,27)$$

is external distribution for $C_1 \cup C_2$ and

$$\mathbf{p} = (1,0,0,0,0,0,0,0,135,315,140,0,630,210,0,0,27)$$

is internal distribution for C.

Unfortunately we cannot obtain nonexistence since $\mathbf{p}$ and $\overline{\mathbf{p}}$ pass all our tests. But repeating the procedure with resudual carrays C_0 and C we collect very rich knowdledge about the structure of $OA(1458,16,3,5)$.

Our investigation is in development but our approach demonstrates effectiveness. We find it perspective.

Chapter 3

Covering radius

Another connection between codes and orthogonal arrays is **covering radius**. The covering radius of an orthogonal array C is the minimum of the numbers ρ such that every point of the Hamming space $H(n, q)$ is within distance ρ of at least one point in C; that is, it is the smallest radius such that closed balls of that radius centered at the points of C have all of $H(n, q)$ as their union (see [10, 11]).
This chapter is based on the paper [5]. After giving some preliminary result, we obtain analytically upper bounds for the covering radius of a given orthogonal array depend on its other parameters and these we have done by investigations of the set of all feasible distance distributions of the corresponding orthogonal arrays. For the special case of a ternary orthogonal array ($q = 3$), using a procedure for reduction of the possible distance distributions of orthogonal array to improve the bound by 1 under certain assumptions.

3.1 Some Preliminaries

One of the important problem for investigation is to find the covering radius of a given orthogonal array. If several orthogonal arrays are available, all with the same parameters (length, alphabet size, strength, cardinality), one way to choose between them is to pick the one with the smallest covering radius. An orthogonal array with a small covering radius has the property that no potential treatment combination is too far from one that is actually used. Several papers by Tietäväinen [44, 43], Laihonen-Litsyn [20, 21], and Fazekas-Levenstein [24] have investigated the relationship between the strength of an orthogonal array to its covering radius.

Definition 3.1.1. *Let C be an orthogonal array $OA(M, n, q, t)$. The* **covering radius** *$\rho(C)$ is the maximal Hamming distance of any potential vector not in the*

array from the closest vector of C, i.e.,

$$\rho(C) := \max_{x \in \mathcal{A}^n} \min_{y \in C} d(x, y).$$

Where $C \subset H_q^n$ is an orthogonal array of strength t. The minimum distance $d(C)$ of C are defined, as usual, by

$$d(C) := \min_{x,y \in C, x \neq y} d(x, y).$$

The relation between the distance distributions of C and its covering radius is based on the following fact. If

$$J := \max\{j : p_0 = \cdots = p_j = 0 \text{ and } p_{j+1} \neq 0\}$$

is the maximum taken over all present distance distributions $\mathbf{p}(\mathbf{x}) = (p_0, p_1, \ldots, p_n)$, $\mathbf{x} \notin C$, then $\rho(C) = J + 1$. If the existence of C is undecided or we know that it exists but it is unknown whether all feasible distance distributions are actually realized, we have the inequality $\rho(C) \leq J + 1$, which is our initial source of upper bounds for $\rho(C)$.

3.2 Bounds for the covering radius

We will work with the system (iv) in Theorem 2.1.2. It is convenient to denote the rows and columns of the matrices bellow from 0 to t and 0 to n, respectively, instead of the usual from 1 to $t + 1$ and 1 to $n + 1$, respectively. So Theorem 2.1.2 (iv) can be written as

$$A_s p^\tau = a, \tag{3.1}$$

where

$$A_s = (a_{ml}) = \left(\binom{l - s}{m} \right)$$

is a $(t + 1) \times (n + 1)$ matrix. The vector $a = (a_0, a_1, \ldots, a_t)^\tau$ is determined by

$$a_m = \frac{M}{q^n} \sum_{i=0}^{n} \binom{n}{i} \binom{i - s}{m} (q - 1)^i,$$

where $m = 0, \ldots, t$. Columns of A_s corresponding to $l = s, \ldots, s + t$ form a $(t + 1) \times (t + 1)$ matrix $R_t = (r_{ij}) = (\binom{j}{i})$. Multiplying the system (3.1) with $R_t^{-1} =$

$((-1)^{i+j}\binom{j}{i})$ (see [26]) we get the system

$$Bp^\tau = b, \tag{3.2}$$

where $B = R_t^{-1}A_s = (b_{ml})$ and $b = R_t^{-1}a = (b_0, \ldots, b_t)^\tau$.

We have already found better expression for the coefficients b_{ml} in Theorem 2.3.1([4]). In contrast, the coefficients b_m do not have one, except for some values of the parameters s and m, like in the next assertion.

Thus $B = (U_1 I_{t+1} U_2)$, where

- $U_1 = (b_{ml})$ is a $(t+1) \times s$ matrix $(l = 0, \ldots, s-1)$;
- $U_2 = (b_{ml})$ is a $(t+1) \times (n-s-t)$ matrix $(l = s+t+1, \ldots, n)$;
- I_{t+1} is the identity $(t+1) \times (t+1)$ matrix, placed in columns $l = s, \ldots, s+t$.

To prove our bounds for covering radius we choose to work with $s = n - t$. This makes the situation simpler, since there is only one matrix U_1 and we write it as U, i.e.

$$Bp^\tau = b, \text{ and } B = (UI_{t+1}) = (b_{ml}), \tag{3.3}$$

where $b = (b_m),\ m = 0, 1, \ldots, t,\ l = 0, 1, \ldots, n$.

We can express now the coefficients b_0 and b_1, which will be needed later.

Corollary 3.2.1. *For given parameters M, n, q, t, $s = n - t$, and $\lambda = M/q^t$ the following hold:*

(i) $b_0 = \lambda\binom{n}{t}$;

(ii) $b_1 = -\lambda\binom{n}{t-1}(n - t - q + 1)$.

Proof. (i) We consecutively obtain

$$\begin{aligned} b_0 &= \lambda q^{t-n} \sum_{i=0}^{n} \binom{n}{i}\binom{n-i}{t}(q-1)^i \quad since \quad m = 0 \\ &= \lambda q^{t-n}\binom{n}{t}\sum_{i=0}^{n}\binom{n-t}{i}(q-1)^i \\ &= \lambda q^{t-n}\binom{n}{t}q^{n-t} \\ &= \lambda\binom{n}{t} \end{aligned}$$

We used the identity $\binom{n}{m}\binom{n-m}{p} = \binom{n}{p}\binom{n-p}{m}$ (see [33]) and $\binom{n-t}{i} = 0$ when $i > n-t$.

(ii) We obtain that

$$\begin{aligned}
b_1 &= \lambda q^{t-n} \sum_{i=0}^{n} \binom{n}{i} \binom{i-n+t}{1} \binom{n-i}{t-1} (q-1)^i \\
&= \lambda q^{t-n} \sum_{i=0}^{n} (i-n+t) \binom{n}{i} \binom{n-i}{t-1} (q-1)^i \\
&= -\lambda q^{t-n} \binom{n}{t-1} \sum_{i=0}^{n} (n-i-t) \binom{n-t+1}{i} (q-1)^i \\
&= -\lambda q^{t-n} \binom{n}{t-1} \left[\sum_{i=0}^{n} (n-t) \binom{n-t+1}{i} (q-1)^i - \sum_{i=0}^{n} i \binom{n-t+1}{i} (q-1)^i \right] \\
&= -\lambda q^{t-n} \binom{n}{t-1} \left[(n-t) q^{n-t+1} - \sum_{i=0}^{n} \binom{n-t+1}{i} \binom{i}{1} (q-1)^i \right] \\
&= -\lambda q^{t-n} \binom{n}{t-1} \left[(n-t) q^{n-t+1} - (n-t+1)(q-1) \sum_{i=0}^{n} \binom{n-t}{i-1} (q-1)^{i-1} \right] \\
&= -\lambda q^{t-n} \binom{n}{t-1} \left[(n-t) q^{n-t+1} - (n-t+1)(q-1) q^{n-t} \right] \\
&= -\lambda q^{t-n} \binom{n}{t-1} (n-t-q+1) q^{n-t} \\
&= -\lambda \binom{n}{t-1} (n-t-q+1).
\end{aligned}$$

We used that $\binom{n}{m}\binom{m}{p} = \binom{n}{p}\binom{n-p}{m-p}$ ([33]) and $\binom{n-t+1}{i} = 0$, if $i > n-t+1$.

□

The next theorem gives the first bounds on covering radius for a given orthogonal array.

Theorem 3.2.2. *Let C be an $OA(M, n, q, t)$ having covering radius $\rho(C)$. Then*

$$\rho(C) \leq n - t.$$

Proof. It is enough to prove that every distance distribution of the type

$$\mathbf{p}(\mathbf{v}) = (\underbrace{0, \ldots, 0}_{n-t}, p_{n-t}, \ldots, p_n)$$

of C has $p_{n-t} \neq 0$. In fact, in this case the system (3.3) has a unique solution of

this type and it is given by

$$\mathbf{p}(\mathbf{v}) = (\underbrace{0, \ldots, 0}_{n-t}, b_0, \ldots, b_{t+1}).$$

It follows from Corollary 3.2.1 (i) that $b_0 = \lambda\binom{n}{t} \neq 0$ whenever $\lambda > 1$ and $n > t$. □

The uniqueness of the solution in the proof of Theorem 3.2.2 allows further improvements.

Theorem 3.2.3. *Let C be an $OA(M, n, q, t)$ having covering radius $\rho(C)$. If $n - t > q - 1$, then*

$$\rho(C) \leq n - t - 1.$$

Proof. Suppose that $\rho(C) = n - t$, i.e. the bound of Theorem 3.2.2 is achieved. Then the only solution of (3.3),

$$\mathbf{p}(\mathbf{v}) = (\underbrace{0, \ldots, 0}_{n-t}, p_{n-t}, \ldots, p_n) = (\underbrace{0, \ldots, 0}_{n-t}, b_0, \ldots, b_{t+1}),$$

is the distance distribution of (every) external point, where the covering radius is realized. Therefore the numbers b_i, $i = 0, \ldots, n$, are integers in the interval $[0, M]$. However, Corollary 3.2.1 (ii) shows that

$$b_1 = -\lambda\binom{n}{t-1}(n - t - q + 1) < 0$$

whenever $n-t > q-1$. This contradicts to our assumption, so the required inequality holds true. □

We present some examples with known orthogonal arrays.

Example 3.2.4. *An $OA(54, 5, 3, 3)$ is shown in ([40]) with distance distribution with maximum number of zeros in the beginning being*

$$(0, 0, 20, 0, 30, 4).$$

Thus $\rho(C) = 2$ which attains the bound of Theorem 3.2.2,

$$\rho(C) \leq n - t = 5 - 3 = 2$$

(note that $n-t = q-1$ here and the argument of Theorem 3.2.3 can not be applied).

Example 3.2.5. *Three constructions of* $OA(18, 7, 3, 2)$ *are described in ([16, 34]). The distance distribution for these OAs with maximum number of zeros in the beginning is*

$$(0, 0, 0, 0, 14, 0, 0, 4),$$

so we have $\rho(C) = 4$. *Now* $n - t = 7 - 2 > 3 - 1 = q - 1$ *and Theorem 3.2.3 can be applied; moreover, its bound is attained in this case,*

$$\rho(C) \leq n - t = 7 - 2 - 1 = 4.$$

3.3 Improvement of the covering radius' bounds

In this section we will use the described already algorithm ([7, 8, 26, 4, 3]) that reduce the possible distance distributions for a given $OA(M, n, q, t)$. The reason is that a given orthogonal array is related with some derived from it orthogonal arrays and some conditions for distance distributions have to be satisfied.

Let C be an $OA(M, n, q, t)$ and we can assume that C contains the all-zero vector. Let $\overset{\mathrm{v}}{C}$ be the orthogonal array obtained from C by deleting the first column. Denote by C_i, $i = 0, 1, \ldots, q-1$ the set obtained by taking all rows of C with the i-th element of $\mathcal{A}$ in the first column and then deleting the first column. (C_0 corresponds to 0 in the first column). Then $\overset{\mathrm{v}}{C}$ is $OA(M, n-1, q, t)$ and C_i is an $OA(M/q, n-1, q, t-1)$.

We compute all possible distance distributions of C, C_i, $\overset{\mathrm{v}}{C}$ using algorithm described in [26], and any other necessary arrays derived from C.

Let $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in C$, i.e., $\mathbf{c}_0 = (c_2, \ldots, c_n) \in C_0$ or C_i. The distance distribution of C with respect to $\mathbf{c}$ is $\mathbf{p}(\mathbf{c}) = (p_0, p_1, \ldots, p_n)$ and the distance distribution of C_0 (or C_i, respectively) with respect to $\mathbf{c}_0$ is $\mathbf{p}^0(\mathbf{c}_0) = (p_0^0, p_1^0, \ldots, p_{n-1}^0)$.

Let us denote the covering radius of C, C_i, $\overset{\mathrm{v}}{C}$ and $C_1 \cup \cdots \cup C_{q-1}$ by $\rho(C), R^i, \overset{\mathrm{v}}{R}$ and $\overline{R}$, respectively. We show an example of how relations between C and its related provide new bounds for $\rho(C)$.

Theorem 3.3.1. *Let* C *be an* $OA(M, n, q, t)$ *with covering radius* $\rho(C)$. *If* $n > 2(t + q - 1)$, *then*

$$\rho(C) \leq n - t - 2.$$

Proof. Since

$$n - t > t + 2(q - 1) > q - 1,$$

Theorem 3.2.3 implies that $\rho(C) \leq n - t - 1$.

Let us assume that equality is attained, i.e. $\rho(C) = n - t - 1$. Thus a distance distribution of C is a solution of the system (3.3) so

$$\mathbf{p}(\mathbf{c}) = (\underbrace{p_0 = 0, \ldots, p_{n-t-2} = 0}_{n-t-1}, \underbrace{p_{n-t-1}, \ldots, p_n}_{t+2}),$$

where $p_{n-t-1} \geq 0$.

It follows from Corollary 2.4.1 (ii) that the above vector $\mathbf{p}(\mathbf{c})$ with deleted first coordinate has to dominate a distance distribution

$$\mathbf{p}^0(\mathbf{c}_0) = (p_0^0, p_1^0, \ldots, p_{n-1}^0)$$

of C_0. This means that there is a distance distribution of C_0 of the form

$$\mathbf{p}^0(\mathbf{c}_0) = (\underbrace{0, \ldots, 0}_{n-t-2}, p_{n-t-1}^0, \ldots, p_{n-1}^0)$$

and the covering radius R^0 is greater than or equal to $n - t - 2$. Note that $\mathbf{p}^0(\mathbf{c}_0)$ is a solution of (3.3) for the parameters of $OA\big(\frac{M}{q}, n-1, q, t-1\big)$ and the same

$$\lambda^0 = \frac{M}{q} \cdot \frac{1}{q^{t-1}} = \lambda.$$

Moreover, we have $p_{n-t-1}^0 = 0$ whence it follows that

$$R^0 = n - t - 1 = \rho(C).$$

Indeed, if we assume that $p_{n-t-1}^0 > 0$, then the distance distribution of $C_1 \cup \cdots \cup C_{q-1}$

$$\begin{aligned}\overline{\mathbf{p}}(c_0) &= (p_1 - p_1^0, \ldots, p_{n-1} - p_{n-1}^0, p_n) \\ &= (\underbrace{0, \ldots, 0}_{n-t-2}, 0 - p_{n-t-1}^0, \ldots, p_{n-1} - p_{n-1}^0, p_n)\end{aligned}$$

will have a negative entry $\overline{p}_{n-t-2} = -p_{n-t-1}^0 < 0$, a contradiction. We note that $C_1 \cup \cdots \cup C_{q-1}$ has parameters $OA\big(\frac{(q-1)M}{q}, n-1, q, t-1\big)$.
Therefore the covering radii of C and C_0 are equal, i.e. $\rho(C) = R^0 = n - t - 1$, and corresponding distance distributions are

$$\mathbf{p}(\mathbf{c}) = (\underbrace{0, \ldots, 0}_{n-t-1}, \underbrace{p_{n-t-1}, \ldots, p_n}_{t+2})$$

for parameters $OA(M, n, q, t)$,

$$\mathbf{p}^0(\mathbf{c}_0) = (\underbrace{0, \ldots, 0}_{n-t-1}, \underbrace{p^0_{n-t}, \ldots, p^0_{n-1}}_{t+1})$$

for parameters $OA(M/q, n-1, q, t-1)$,

$$\overline{\mathbf{p}}(\mathbf{c}_0) = (\underbrace{0, \ldots, 0}_{n-t-2}, \underbrace{p_{n-t-1}, p_{n-t} - p^0_{n-t}, p_n, \ldots, p_{n-1} - p^0_{n-1}, p_n}_{t+2})$$

for parameters $OA\left(\frac{(q-1)M}{q}, n-1, q, t-1\right)$ and

$$\overline{\lambda} = \frac{\frac{(q-1)M}{q}}{q^{t-1}} = (q-1)\lambda.$$

The distance distribution $\overline{\mathbf{p}}(\mathbf{c}_0)$ of $C_1 \cup \cdots \cup C_{q-1}$ is a solution of the corresponding system (3.3) for these parameters, which we denote by $\overline{B}\overline{p}^\tau = \overline{b}$. The first equation of this system is

$$\overline{b}_{0,n-t-2}\overline{p}_{n-t-2} + \overline{b}_{0,n-t-1}\overline{p}_{n-t-1} + \overline{p}_{n-t} = \overline{b}_0, \tag{3.4}$$

where

$$\overline{p}_{n-t-2} = p_{n-t-1},\ \overline{p}_{n-t-1} = p_{n-t} - p^0_{n-t},$$

$$\overline{p}_{n-t} = p_{n-t+1} - p^0_{n-t+1},$$

and

$$\overline{b}_0 = (q-1)\lambda\binom{n-1}{t-1}$$

from Corollary 3.2.1 (i) for $C_1 \cup \cdots \cup C_{q-1}$.

Let us denote $p_{n-t-1} = x$ for short. Our goal is to express and to show that the number $\overline{p}_{n-t} = x - p^0_{n-t+1}$ is negative under the assumption $n > 2(t+q-1)$, obtaining this way the desired contradiction. We find the remaining parameters from first equations of the system (3.3) written for the corresponding parameters as follows.

First p_{n-t} is expressed from the first equation of system (3.3) for parameters $OA(M, n, q, t)$, i.e. we have

$$b_{0,n-t-1}x + p_{n-t} = b_0$$

which is equivalent to

$$(t+1)x + p_{n-t} = \lambda\binom{n}{t}.$$

Therefore

$$p_{n-t} = \lambda\binom{n}{t} - (t+1)x.$$

Since $p_{n-t} \geq 0$, we upperbound x by

$$x \leq \frac{\lambda\binom{n}{t}}{t+1} = \frac{\lambda n}{t(t+1)}\binom{n-1}{t-1}.$$

Next, p^0_{n-t} is found from the first equation in the system (3.3) for parameters $OA(M/q, n-1, q, t-1)$, i.e.

$$p^0_{n-t} = b^0_0 = \lambda\binom{n-1}{t-1}.$$

We substitute in (3.4) and obtain the equation

$$\frac{t(t+1)}{2}x + t\left(\lambda\binom{n}{t} - (t+1)x - \lambda\binom{n-1}{t-1}\right) + p_{n-t+1} - p^0_{n-t+1} = (q-1)\lambda\binom{n-1}{t-1}.$$

After simplifications we obtain

$$\begin{aligned}\overline{p}_{n-t} &= p_{n-t+1} - p^0_{n-t+1} \\ &\leq \frac{\lambda}{2}\binom{n-1}{t-1}\Big(2t + 2(q-1) - n\Big).\end{aligned}$$

It is obvious now that the inequality $n > 2(t+q-1)$ from the theorem's condition implies $\overline{p}_{n-t} < 0$. This contradicts to the assumption that $\rho(C) = n-t-1$, so we conclude that $\rho(C) \leq n-t-2$. □

We again present examples with known orthogonal arrays.

Example 3.3.2. *For $OA(27, 13, 3, 2)$ a construction in [40] shows that the distance distribution with maximum number of zeros in the beginning is*

$$[0, 0, 0, 0, 0, 0, 0, 13, 0, 0, 13, 0, 0, 1],$$

so $\rho(C) = 7$. *For these parameters the bound of Theorem 3.3.1 gives*

$$\rho(C) \leq 13 - 2 - 2 = 9.$$

Example 3.3.3. *For* $OA(36, 13, 3, 2)$ *a construction in [40] gives a distance distribution with maximum number of zeros in the beginning as*

$$[0, 0, 0, 0, 0, 0, 0, 10, 14, 0, 6, 4, 0, 2],$$

so $\rho(C) = 7$. *For these parameters the bound of Theorem 3.3.1 is*

$$\rho(C) \leq 13 - 2 - 2 = 9.$$

Example 3.3.4. *For* $OA(729, 14, 3, 4)$ *a construction in [40] shows that the distance distribution with maximum number of zeros in the beginning is*

$$[0, 0, 0, 0, 0, 14, 42, 42, 133, 126, 210, 70, 84, 0, 8],$$

so $\rho(C) = 5$. *For these parameters the bound of Theorem 3.3.1 gives*

$$\rho(C) \leq 14 - 4 - 2 = 8.$$

In conclusion we can say that the technique we use looks promising but further restrictions should be added. For example, combination of extensive use of the methods from [7] and [8] and the observation $\rho(C) \leq J + 1$ from the beginning can produce good bounds in many particular cases.

Bibliography

[1] Bose, R., and Bush, K. Orthogonal arrays of strength two and three. *Ann. Math.Stat. 23* (1952), 508–524.

[2] Boumova, S., Marinova, T., Ramaj, T., and Stoyanova, M. Nonexistence of (17, 108, 3) ternary orthogonal array. *Annuaire de l'Université se Sofia "St. Kl. Ohridski" Faculté de Mathématiques et Informatique, Ann. Sofia Univ., Fac. Math and Inf. 106* (2019), 117–126.

[3] Boumova, S., Marinova, T., and Stoyanova, M. On ternary orthogonal arrays. *Proceedings of 17th International Workshop on Algebraic and Combinatorial Coding Theory* (2018), 102–105.

[4] Boumova, S., Ramaj, T., and Stoyanova, M. Computing distance distributions of ternary orthogonal arrays. *BGSIAM* (2019).

[5] Boumova, S., Ramaj, T., and Stoyanova, M. On covering radius of orthogonal arrays. *Proceedings of 16th International Workshop on Algebraic and Combinatorial Coding Theory* (2020).

[6] Boumova, S., Ramaj, T., and Stoyanova, M. Computing distance distributions of ternary orthogonal arrays. *Comptes rendus de l'Académie bulgare des Sciences* (to appear).

[7] Boyvalenkov, P., and Kulina, H. Investigation of binary orthogonal arrays via their distance distributions. *Problems of Information Transmission 14* (1998), 97–107.

[8] Boyvalenkov, P., Marinova, T., and Stoyanova, M. Nonexistence of a few binary orthogonal arrays. *Discrete Applied Mathematics 2* (2017), 144–150.

[9] Bush, K. A. *Orthogonal arrays.* PhD thesis, University of North Carolina, 1950.

[10] Cohen, G., Honkala, I., Litsyn, D., and Lobstain, A. *Covering codes.* North-Holland Mathematical Library, vol. 54, ELSEVIAR, 1997.

[11] Cohen, G., Karpovsky, M., Matson, H., and Schatz, J. Covering radius – survey and recent results. *IEEE Trans. Infor. Theory IT-311* (May 1985), no 3.

[12] Delsarte, P. Bounds for unrestricted codes by linear programming. *Philips Research Reports 27* (1972), 272–289.

[13] Delsarte, P. An algebraic approach to the association schemes of coding theory. *Philips Research Reports Supplements 10* (1973).

[14] Delsarte, P. Four fundamental parameters of a code and their combinatorial significance. *Inform. Contr. 23* (1973), 407–438.

[15] Delsarte, P., and Levensthein, V. Association schemes and coding theory. *IEEE Trans. on Inform. Theory 44*, 6 (1998), 2477–2504.

[16] Evangelaras, H., Koukouvinos, C., and Lappas, E. 18-run nonisomorphic three level orthogonal arrays. *Metrika 66* (2007), 437–449.

[17] Hedayat, A., Sloane, N., and Stufken, J. *Orthogonal Arrays: Theory and Applications.* Springer-Verlag, New York, 1999.

[18] James, G., and Liebeck, M. *Representations and Characters of Groups (2nd ed.).* Cambridge University Press.

[19] Krawtchouk, M. Sur une généralisation des polynômes d' hermite. *Compt.rend. 189*.

[20] Laihonen, T., and Litsyn, S. On upper bounds for minimum distance and covering radius of non-binary codes. *Designs, Codes, Crypt.. 14* (1998), 71–80.

[21] Laihonen, T., and Litsyn, S. New bounds on covering radius as a function of dual distance. *SIAM J. Discrete Math 12* (1999), 243–251.

[22] Levenshtein, V. I. Krawtchouk polynomials and universal bounds for codes and designs in hamming spaces. *IEEE Trans. Inform. Theory 41, no 5* (1995), 1303–1321.

[23] Levenshtein, V. I. Universal bounds for codes and design in *handbook of coding theory, eds. v.pless and w.c.huffman.* Elsevier Science B.V. *(1998), 499–648.*

[24] Levenshtein, V. I., and G., F. *On upper bounds for code distance and covering radius of designs in polynomial metric spaces.* Journal of Combinatorial Theory Series A 70 *(1995), 267–288.*

[25] MacWIlliams, F. J., and Sloane, N. J. A. *The theory of error-correcting codes.* Amsterdam, The Netherlands: North Holland *(1997).*

[26] Manev, N. L. *On the distance distributions of orthogonal arrays.* Problems of Information Transmission 56*, 5 (2020).*

[27] Panario, D., Saaltink, M., Stevens, B., and Wevrick, D. *A general construction of ordered orthogonal arrays using lfsrs.* IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 65, NO. 7 *(JULY 2019), 4316– 4326.*

[28] Pless, V., and Huffman, W. Handbook of Coding Theory*. North-Holland, 1998.*

[29] Raghavarao, D. Constructions and Combinatorial Problems in Design of Experiments*. Wiley, 1st Edition, 1971.*

[30] Rao, C. R. *Hypercubes of strength d leading to confounded designs in factorial experiments.* Bull. Calcutta Math. Soc. 38 *(1946), 67–78.*

[31] Rao, C. R. *Factorial experiments derivable from combinatorial arrangements of arrays.* Royal Statist. Soc. (Suppl.) 9 *(1947), 128–139.*

[32] Rao, C. R. *On a class of arrangements.* Proc. Edinburgh Math. Soc. 8 *(1949), 119–125.*

[33] Riordan, J. *Combinatorial identities.* John Wiley& Sons, Inc. *(1968).*

[34] Schoen, E. D., Eendebak, P., and Nguyen, M. *Complete enumeration of pure-level and mixed-level orthogonal arrays.* Journal of Combinatorial Designs 18, Issue 2 *(2010), 123–140.*

[35] Seiden, E. *On the problem of construction of orthogonal arrays.* Ann. Math. Statist. 25 *(1954), 151–156.*

[36] Seiden, E. *On the maximum number of constraints of an orthogonal array.* he Annals of Mathematical Statistics, 26 *(1955), 132–135.*

[37] Shahriari, S. Algebra in Action, A course in groups, rings, and fields. *American Mathematical Society.*

[38] Shannon, C. E. *A mathematical theory of communication.* Bell. Syst. Tech. J. 27 *(1948), 374–423, 623–656.*

[39] Shannon, C. E. *Collected papers.* New York: IEEE Press. Edited by Sloane, N. J. A. and Wyner, A. D. *(1992).*

[40] Sloane, N. J. A. *http://neilsloane.com/oadir/index.html.*

[41] Szego, G. Orthogonal polynomials. *Providence, AMS col. publ., 1939.*

[42] Tang, Y., Xu, H., and Lin, D. K. J. *Uniform fractional factorial designs.* Annals of Statistics 40*, 2 (04 2012), 891–907.*

[43] Tietäväinen, A. *Covering radius and dual distance. Des. Codes Cryptogr (May 1991), 1:31–46.*

[44] Tietäväinen, A. *An upper bound on the covering radius as a function of the dual distance. IEEE Trans. Inform. Theory 36(6) (Nov 1990), 1472–1474.*

[45] Torres-Jimenez, J., Avila-George, H., Rangel-Valdez, N., and Gonzalez-Hernandez, L. *Construction of orthogonal arrays of index unity using logarithm tables for galois fields.* Cryptography and Security in Computing, Ch. 4*, 71–90.*