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

Tedis Ramaj

Algebraic methods for studying some combinatorial configurations and their applications

ABSTRACT

of a Ph.D. 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

Sofia, 2021

The Ph.D. Thesis has 88 pages and consists of an introduction, three chapters and a bibliography with 45 titles of papers.

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 array exist?

⋆ **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), 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 (Theorem 2.1.2 (i), (ii), (iii), (iv)) 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) 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) 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 3.2.3**) 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 Assoc. Prof. Silvia Boumova, PhD and Assoc. Prof. Maya Stoyanova, PhD for their valuable advices, guidance and help.

I would like to thank all colleagues from the Department of Algebra of Faculty of Mathematics and Informatics, Sofia University "St. Kliment Ohridski" for 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

pleasant and stimulating atmosphere during the preparation of the 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 $OA(108, 18, 3, 3)$ and $(108, 17, 3, 3)$ ternary orthogonal arrays. The result of nonexistence of $OA(108, 18, 3, 3)$ 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.

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 Levenstein, 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.*