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

Tanya Todorova Marinova

ALGORITHMS FOR CHARACTERISATION OF ORTHOGONAL ARRAYS

ABSTRACT

of a Ph.D. Thesis
for awarding the Ph.D. degree
in the Professional field 4.5 Mathematics
Doctoral program "Algebra, topology and applications"

supervisor:
Assoc. Prof. Maya Stoyanova, Ph.D.

Sofia
2021

The Ph.D. Thesis has 115 pages and consists of an introduction, four chapters and a bibliography with 59 titles of papers.

The numbering of the definitions, theorems and corollaries in this abstract follows the one in the Ph.D. thesis.

In the Ph.D. thesis the structure of some classes of orthogonal arrays in the Hamming space $H(n,q)$ has been investigated. Orthogonal arrays have numerous applications in various subfields of mathematics, such as statistics [30, 48, 56], coding theory [1, 2, 20, 29], and cryptography [4, 36, 57]. Moreover, they have applications in computer science and physics as well.

The research in the thesis is performed in the Hamming space $H(n,q)$, considered as a finite polynomial metric space. Polynomial techniques [21, 37, 38, 13] were used to study the distance distribution of orthogonal arrays and to obtain some constraints on the structure of the arrays.

The Hamming space is the space of all n-tuples over the alphabet (field) Q with q elements. The dimension of $H(n,q)$ is exactly n. In $H(n,q)$ a Hamming metric is introduced using the distance $d(x,y)$, between two words of the space $x,y \in H(n,q)$, which is defined as the number of coordinates in which the two words differ. An inner product is introduced according to the following rule:

$$\langle x,y\rangle := 1 - \frac{2d(x,y)}{n}.$$

The reversible function $\sigma(d) = 1 - \frac{2d}{n}$ is called standard substitution. We use it to convert between distances and inner products $\sigma^{-1}(d) = 1 - \frac{2d}{n}$.

The first chapter of the thesis presents in detail the Krawtchouk polynomials and the normalized Krawtchouk polynomials, which are the zonal polynomials of the finite metric space $H(n,q)$.

Any non-empty (finite) subset $C \subset H(n,q)$ is called a code. The most important parameters of a code are its dimension n, its cardinality $M = |C|$, as well as the minimum distance between two different words in it $d = d(C) = \min\{\ d(x,y)\ :\ x,y \in C, x \neq y\}$.

Fazekas and Levenstein introduced the term τ-design in $H(n,q)$.

Definition 1.1.1 *A code $C \subset H(n,q)$ is called a τ-design if and only if for every polynomial with real coefficients $f(t)$ of degree $k \leq \tau$ and for every point $y \in H(n,q)$ the equality*

$$\sum_{x\in C} f(\langle x,y\rangle) = f_0|C|,$$

holds where f_0 is the first coefficient in the expansion of the polynomial $f(t)$ on the normalized Krawchouk polynomials, i.e. $f(t) = \sum_{i=0}^{n} f_i Q_i^{(n)}(t)$.

The maximal non-negative integer $\tau \leq n$ for which C is a τ-design is called the strength of the design. Considered as combinatorial structures, the τ-designs are shown to be exactly the orthogonal arrays in $H(n,q)$.

Definition 1.2.1 *Let Q be an arbitrary alphabet (field) with q elements, and C be a matrix with M rows and n columns with elements of Q. We will say that C is an orthogonal array with q levels, strength τ and index λ, where $0 \leq \tau \leq n$, if each $M \times \tau$ submatrix of C contains all τ tuples over Q exactly λ times as rows. We will denote such an orthogonal array C by (n, M, q, τ).*

In Paragraph 1.2 the main properties of orthogonal arrays are presented. Some of their characteristics are introduced. The main characteristic in this thesis is the distance distribution of an orthogonal array with respect to a point of the Hamming space.

Definition 1.2.2 *For every (n, M, q, τ) orthogonal array $C \subset H(n, q)$ and for a fixed point $c \in H(n, q)$ we consider the $(n+1)$-tuple of non-negative integers*

$$W = W(c) = (w_0(c), w_1(c), \ldots, w_n(c)),$$

where

$$w_i(c) = |\{x \in C | d(x, c) = i\}|,$$

for $i = 0, \ldots, n$. We call $W = W(c)$ the distance distribution of the orthogonal array C with respect to the point c (or the distance distribution of the point c when the array C is implied).

In this work we will use different notations depending on whether the point c belongs to the array C or not. More precisely, for an internal point $c \in C$ we will denote the distance distribution of C with respect to the point c by

$$P = P(c) = (p_0 \geq 1, p_1, \ldots, p_n),$$

whereas for an external point $c \in H(n, q) \setminus C$ we will denote the distance distribution of C with respect to the point c by

$$Q = Q(c) = (q_0 = 0, q_1, \ldots, q_n).$$

The research investigates orthogonal arrays and their combinatorial properties using known polynomial techniques on τ-designs in polynomial metric spaces.

The main problem of coding theory, investigated in this work, is the following:

Problem 1.3.1 *Find the minimal possible value for the cardinality M such that an orthogonal array (n, M, q, τ) exists in $H(n, q)$ for a fixed strength τ, columns n and levels q, in other words to evaluate*

$$B(n, q, \tau) = \min\{M = |C| \ : \ \textit{exists } (n, M, q, \tau) \textit{ orthogonal array in } H(n, q)\}.$$

It is known that the index λ of an orthogonal array can be calculated using the formula $\lambda = M/q^\tau$. This means that we can restate the previous problem as follows.

Problem 1.3.2 *Find the minimal possible value for the index λ such that an orthogonal array (n, M, q, τ) exists in $H(n, q)$ for a fixed strength τ, columns n and levels q, in other words to evaluate*

$$\Lambda(n, q, \tau) := min\{\lambda = |C|/q^\tau \ : \ \textit{exists} \ \ (n, M, q, \tau) \textit{ orthogonal array}\}.$$

Paragraph 1.3 describes well-known bounds for the cardinality of an orthogonal array $C \in H(n, q)$. These are the linear programming bound (or Delsarte bound)[24], the Rao bound and the Hamming bound [49], [39] which in the Hamming space $H(n, q)$ coincide. Singleton bound [53] and Plotkin bound [47] are also introduced. The latter one is valid for the binary Hamming space $H(n, 2)$. Levenshtein's universal bounds (upper and lower) are described in detail. [38].

Finding all the possibilities for different characteristics of a code is a standard technique in coding theory and in combinatorics. The idea of finding the distance distributions of optimal codes and designs was first introduced by Delsarte in his Ph.D. thesis [21]. We will apply one of the ways to calculate all the possibilities for the distance distribution of a (n, M, q, τ) orthogonal array. This is a corollary of a more general approach proposed by Boyvalenkov [9].

More precisely, the following theorem gives us the necessary technique for the initial calculation of all the possibilities for the distance distribution with respect to an internal or an external point for an orthogonal array with fixed parameters.(see [13], [14]).

Theorem 1.4.1 *Let $C \subset H(n,q)$ be a (n, M, q, τ) orthogonal array and let $c \in H(n,q)$ be fixed. Then*

(a) if $c \in C$, the distance distribution of C with respect to c satisfies the system

$$\sum_{i=0}^{n} p_i \left(1 - \frac{2i}{n}\right)^k = b_k |C|, \quad k = 0, 1, \ldots, \tau, \tag{1}$$

(b) if $c \notin C$, the distance distribution of C with respect to c satisfies the system

$$\sum_{i=1}^{n} q_i \left(1 - \frac{2i}{n}\right)^k = b_k |C|, \quad k = 0, 1, \ldots, \tau, \tag{2}$$

where b_k is the first coefficient in the expansion of the polynomial t^k in terms of the normalised Krawtchouk polynomials, i.e. $t^k = b_k + \sum_{i=1}^{k} P_i^{(n)}(t)$.

Using **Theorem 1.4.1** we find the sets of all the possible distance distributions with respect to internal and external (for the array) points. For fixed n, M, $\tau \leq n$ and q we denote the set of all possible distance distributions with respect to an arbitrary internal point by $P(n, M, q, \tau)$, and the set of all possible distance distributions with respect to an arbitrary external point - $Q(n, M, q, \tau)$. The set of all possible distance distributions regardless of the selected point is denoted by

$$W(n, M, q, \tau) = P(n, M, q, \tau) \cup Q(n, M, q, \tau).$$

The next theorem gives us the opportunity to fix a point of the space and work on it without loss of generality.

Theorem 1.4.4 *The set $W(n, M, q, \tau)$ is exactly the set of distance distributions of the orthogonal arrays with parameters (n, M, q, τ) with respect to the point $\mathbf{0} \in H(n,q)$.*

Theorem 1.4.6 and **Theorem 1.4.8** are also proved as well as their immediate corollaries. This allow us to consider the distance distributions of orthogonal arrays with respect to any fixed point of the space $H(n,q)$.

In the second chapter, orthogonal arrays in the binary Hamming space $H(n,2)$ are considered. Note that $H(n,2)$ is an antipodal metric space, i.e. for each point $x \in H(n,2)$ there is an unique $\bar{x} \in H(n,2)$ for which the condition $d(x, \bar{x}) = n$ is fulfilled. Using this fact, in [28] we prove that orthogonal arrays with parameters $(n, M, 2, 2k)$ and $(n+1, 2M, 2, 2k+1)$ exist simultaneously.

The thesis uses two main constructions for the study of orthogonal arrays. In the first construction for an orthogonal array with fixed parameters $(n, M, 2, \tau)$, we cut off an arbitrary column and analyse the connections between the distance distributions of the original and of the newly obtained arrays. In this construction the derived orthogonal arrays have parameters $(n-1, M, 2, \tau)$ and $(n-1, M/2, 2, \tau-1)$. The construction has the following form.

$$\overbrace{\begin{array}{|c|c|}\hline 0 & \\ 0 & Y=(y_0,y_1,\ldots,y_{n-1}) \\ \vdots & C_0-(n-1,M/2,2,\tau-1) \\ 0 & \\ \hline 1 & \\ 1 & X=(x_1,x_2,\ldots,x_n) \\ \vdots & C_1-(n-1,M/2,2,\tau-1) \\ 1 & \\ \hline \end{array}}^{\begin{array}{c}C'-(n-1,M,2,\tau)\\ W'=(w'_0,w'_1,\ldots,w'_{n-1})\end{array}}$$

$$\begin{array}{c}C-(n,M,2,\tau)\\ W=(w_0,w_1,\ldots,w_n)\end{array}$$

Construction 2.3.

In Paragraph 2.3 the set of distance distributions with respect to an internal point $P(n, M, 2, \tau)$ is investigated. Using **Theorem 2.3.1**, **Theorem 2.3.3**, **Theorem 2.3.4** and **Theorem 2.3.6** an algorithm for reducing the elements in $P(n, M, 2, \tau)$ is described.

When working only with internal points, some of the orthogonal arrays obtained in Construction 2.2 cannot be analysed. Therefore, in Paragraph 2.4 the theorems in Paragraph 2.3 are generalised on the set of distance distributions $W(n, M, 2, \tau)$ with respect to any arbitrary point of the space $H(n, 2)$. In addition, the distance distributions of the derived orthogonal arrays are described.

Theorem 2.3.4 *Let $C \subset H(n,2)$ be a $(n, M, 2, \tau)$ binary orthogonal array with distance distribution $W \in W(n, M, \tau, 2)$ with respect to an arbitrary point $c \in H(n,2)$. Let $c' \in H(n-1,2)$ and C' be obtained from c and C by Construction 2.3, and let $W' \in W(n-1, M, 2, \tau)$ be the distance distribution of the array C' with respect to the point c'. The system of linear equations*

$$\left|\begin{array}{l} x_i + y_i = w_i,\ i = 1,2,\ldots,n-1 \\ x_{i+1} + y_i = w'_i,\ i = 0,1,\ldots,n-1 \\ y_0 = w_0 \\ x_n = w_n \\ x_i, y_i \in \mathbb{Z},\ x_i \geq 0,\ y_i \geq 0,\ i = 0,1,\ldots,n \end{array}\right. . \tag{3}$$

with variables $X = (x_1, x_2, \ldots, x_{n-1}, x_n)$ and $Y = (y_0, y_1, \ldots, y_{n-1})$ has the unique solu-

tion:

$$X = (w_0' - w_0, \sum_{j=0}^{1}(w_j' - w_j), \ldots, \sum_{j=0}^{n-2}(w_j' - w_j), w_n),$$

$$Y = (w_0, w_1 - (w_0' - w_0), w_2 - \sum_{j=0}^{1}(w_j' - w_j), \ldots, w_{n-1} - \sum_{j=0}^{n-2}(w_j' - w_j)).$$

In the same Paragraph, using the antipodallity of $H(n,2)$, we outline proofs for some important theorems and corollaries. Using those we succeed in proving the important for our research **Theorem 2.4.16**. This theorem gives us the distance distribution (with respect to an arbitrary point x of space) of the orthogonal array with the same parameters $(n, M, 2, \tau)$ which is isomorphic to C. Thus, we came to the conclusion that a given distance distribution of an array, i.e. element of the set $W(n, M, 2, \tau)$, depends on another distance distribution (element) of the same set.

A second algorithms is described in the thesis. It is used to reduce the set of distance distributions with respect to an arbitrary point $W(n, M, 2, \tau)$. This algorithm is generally more powerful than Algorithm 1, but the main disadvantage is that the cardinality of $W(n, M, 2, \tau)$ is greater than the cardinality of the set $P(n, M, 2, \tau)$ for big n.

A second construction is considered in Paragraph 2.5 - two columns from the fixed orthogonal array C are cut off. We obtain numerous orthogonal arrays with different parameters: $(n-1, M, 2, \tau)$, $(n-2, M, 2, \tau)$, $(n-1, M/2, 2, \tau)$, $(n-2, M/2, 2, \tau)$, as well as several other orthogonal arrays with the same parameters as the original array $(n, M, 2, \tau)$. The different connections between their distance distributions are proved in detail in Theorems **2.5.3 - 2.5.28**. Where possible the distance distributions are explicitly provided. A third algorithm has been developed that improves the results for reducing the set of distance distributions $W(n, M, 2, \tau)$.

We should note that the results in the present work depend on the implementation of the algorithms. Therefore, a number of optimizations that improve the performance of our programs have been described in this thesis.

In Paragraph 2.8 all nonexistence results are described. Those are obtain by using the previously mentioned algorithms.

Theorem 2.8.1 *A binary orthogonal array with parameters* $(4, 96, 11)$ *does not exist.*

Theorem 2.8.2 *A binary orthogonal array with parameters* $(4, 96, 10)$ *does not exist.*

The following results were also obtained.

Corollary 2.8.3 *Binary orthogonal arrays with parameters* $(11, 192, 5)$ *and* $(12, 192, 5)$ *do not exist.*

Using Algorithm 2 the previous described results were improved upon.

Theorem 2.8.4 *A binary orthogonal array with parameters* $(9, 96, 2, 4)$ *does not exist.*

Corollary 2.8.5 *A binary orthogonal array with parameters* $(10, 192, 2, 5)$ *does not exist.*

Another series on which the algorithms were applied is $(13, 224, 2, 5)$. On this input Algorithm 1 gives the following result.

Theorem 2.8.6 *A binary orthogonal array with parameters* $(13, 224, 2, 5)$ *does not exist.*

Corollary 2.8.7 *A binary orthogonal array with parameters* $(12, 112, 2, 4)$ *does not exist.*

Applying Algorithm 2 the following theorem and its corollaries are obtained.

Theorem 2.8.8 *A binary orthogonal array with parameters* $(10, 112, 2, 4)$ *does not exist.*

Corollary 2.8.9 *A binary orthogonal array with parameters* $(11, 112, 2, 4)$ *does not exist.*

Corollary 2.8.10 *A binary orthogonal array with parameters* $(11, 224, 2, 5)$ *does not exist.*

Corollary 2.8.11 *A binary orthogonal array with parameters* $(12, 224, 2, 5)$ *does not exist.*

In order to obtain a complete result on the considered series, it was necessary to use the most powerful, but also the slowest of the described algorithms, namely Algorithm 3. The following results were obtained.

Theorem 2.8.12 *A binary orthogonal array with parameters* $(9, 112, 2, 4)$ *does not exist.*

Corollary 2.8.13 *A binary orthogonal array with parameters* $(10, 224, 2, 5)$ *does not exist.*

Some already known results were also described. In this way we reached the exact bounds for $\Lambda(n, 2, \tau)$ in the following cases:

$$\Lambda(9, 2, 4) = \Lambda(10, 2, 5) = 8, \quad \Lambda(9, 2, 4) = \Lambda(10, 2, 5) = 8,$$

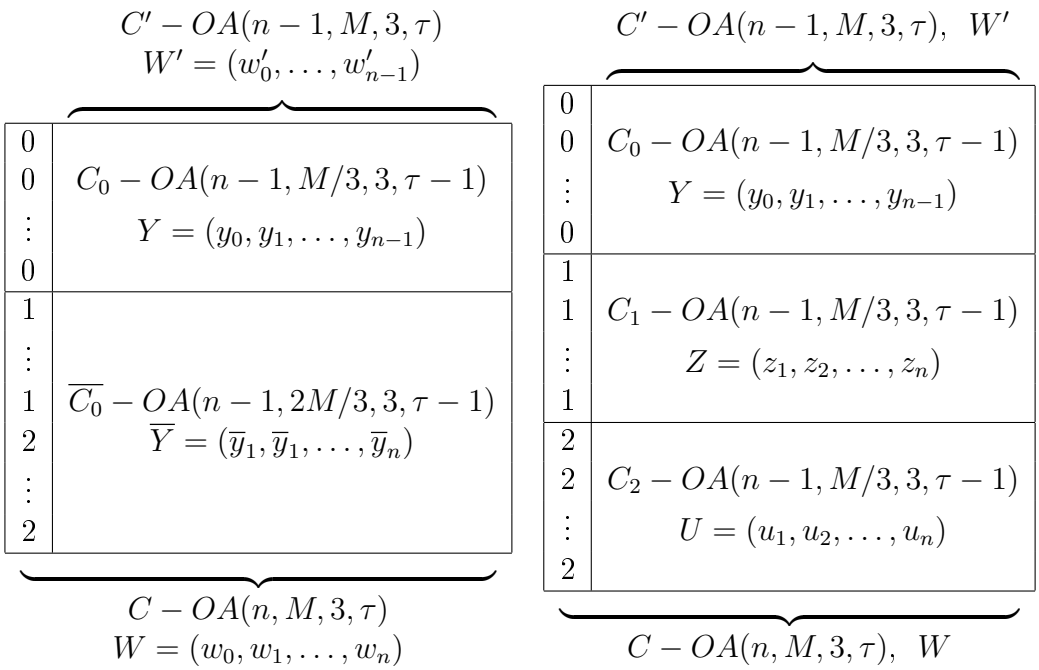
$$\Lambda(11, 2, 4) = \Lambda(12, 2, 5) = 8 \quad \Lambda(12, 2, 5) = \Lambda(13, 2, 5) = 8.$$

Based on the outlined algorithms, we were able to achieve other already known results for nonexistence. These are described at the end of Paragraph 2.8. Although we have not achieved a result for existence or nonexistence, we have obtained a significant reduction in the number of elements in the set $W(n, M, 2, \tau)$ of possibilities for distance distributions of the studied orthogonal array.

The second chapter is based on the following three publications [16], [17] and [43].

In the third chapter, orthogonal arrays over the ternary Hamming space $H(n, 3)$ are investigated. The sets of distance distributions $W(n, M, 3, \tau)$ and $P(n, M, 3, \tau)$ are analysed. An analogous (to the first in the binary case) construction with the removal of one column from a ternary orthogonal array with fixed parameters $(n, M, 3, \tau)$ is described. This construction is illustrated for $\ell = 1$ below.

As can be seen, several derived orthogonal arrays with parameters $(n-1, M, 3, \tau)$, $(n-1, M/3, 3, \tau-1)$ and $(n-1, 2M/3, 3, \tau-1)$ are obtained from the orthogonal array C. For these orthogonal arrays, connections can be found between their distance distributions and the distance distribution of the fixed orthogonal array C. Theorem 3.2.2 gives us the distance distributions of some of the investigated orthogonal arrays. **Theorem 3.2.6** gives a linear system that should be satisfied by the distance distributions of the orthogonal arrays $(n-1, M/3, 3, \tau-1)$ and $(n-1, 2M/3, 3, \tau-1)$.



Construction 3.2 (Figure 1).

Let us denote the three transpositions from the symmetric group S_3 by $\sigma_0 = (12)$, $\sigma_1 = (20)$ and $\sigma_2 = (01)$, respectively. Let us denote the two cycles by $\rho = (012)$ and $\rho^2 = (021)$, respectively. By the properties of orthogonal arrays if we permute the elements in a fixed column we will obtain an orthogonal array with parameters $(n, M, 3, \tau)$. If we first apply the three transpositions on the fixed ℓ^{th} column of the orthogonal array C with distance distribution $W \in W(n, M, 3, \tau)$ with respect to the point $c \in H(n, 3)$, we get three isomorphic to C orthogonal arrays with parameters $(n, M, 3, \tau)$. Let us denote these arrays by C^{σ_0}, C^{σ_1} and C^{σ_2}, respectively. In fact, the result of applying the permutation $\sigma_0 = (12)$ over C results in the orthogonal array with the same distance distribution W with respect to the point c of C. The distance distributions of the other two orthogonal arrays obtained by permutations σ_1, σ_2 we denote by W^{σ_1} and W^{σ_2}, respectively. Applying one of the cycles in S_3 over the ℓ^{th} column of C results in an orthogonal array isomorphic to one of the known ones with the same parameters.

The following theorem describes the distance distribution of the derived orthogonal arrays.

Theorem 3.2.7 *Let $C \subset H(n, 3)$ be a $(n, M, 3, \tau)$ ternary orthogonal array, such that*

$$\begin{aligned} W &= (w_0, w_1, \ldots, w_n) = (y_0, y_1 + \overline{y}_1, \ldots, y_{n-1} + \overline{y}_{n-1}, \overline{y}_n) \\ &= (y_0, y_1 + z_1 + u_1, \ldots, y_{n-1} + z_{n-1} + u_{n-1}, z_n + u_n) \in W(n, M, \tau), \end{aligned}$$

is the distance distribution of C with respect to an arbitrary point $c \in H(n, 3)$. Then:

(a) The distance distribution $W^{\sigma_1} \in W(n, M, \tau)$ of the ternary orthogonal array C^{σ_1} with respect to the point c is

$$W^{\sigma_1} = (u_1, y_0 + z_1 + u_2, \ldots, y_{n-2} + z_{n-1} + u_n, y_{n-1} + z_n);$$

(b) The distance distribution $W^{\sigma_2} \in W(n, M, \tau)$ *of the ternary orthogonal array* C^{σ_2} *with respect to the point* c *is*

$$W^{\sigma_2} = (z_1, y_0 + u_1 + z_2, \ldots, y_{n-2} + u_{n-1} + z_n, y_{n-1} + u_n).$$

We formulated and proved **Theorem 3.2.10**, which is analogous to the binary case **Theorem 2.4.18**. Based on **Theorems 3.2.2-3.2.10** in Paragraph 3.2 an algorithm for reducing the elements of the set $W(n, M, 3, \tau)$ is described.

When trying to generate the set $W(n-1, 2M/3, 3, \tau-1)$, we established that even for relatively small parameters it has a very large cardinality. Even the set $P(n-1, 2M/3, 3, \tau-1)$ proves to be of a substantial size. That is the reason why in Paragraph 3.3 we describe another algorithm. Its input is the set of the distance distributions with respect to an internal point $P(n, M, 3, \tau)$. By applying this algorithm the following theorem is proven.

Theorem 3.3.1 *A ternary orthogonal array with* $(17, 108, 3, 3)$ *does not exist.*

In this way we conclude that in the ternary case we have $5 \leq \Lambda(17, 3, 3)$.

The third chapter is based on the following two publications: [6] and [7].

In the last forth chapter we introduce the concept of energy of orthogonal arrays in the Hamming space $H(n, q)$.

Definition 4.0.2 *Let* C *be an orthogonal array (design) in* $H(n, q)$ *with parameters* (n, M, q, τ). *For each function (potential)* $h(t) : [-1, 1] \to (0, +\infty)$ *we define* h*-energy (or potential energy) of the orthogonal array* C *as follows:*

$$\mathcal{E}(n, C; h) := \frac{1}{|C|} \sum_{x,y \in C, x \neq y} h(\langle x, y \rangle).$$

The two main problems when working with energies of orthogonal arrays aim to find the minimum and the maximum value of the energy when the potential function h is fixed.

Problem 4.0.3 *Let the potential function* h, *the length of the vectors* n, *the strength* τ *and the cardinality* $|C| = M = \lambda q^{\tau}$ *be fixed. Find the minimum possible energy* $\mathcal{L}(n, M; \tau; h)$, *such that an orthogonal* (n, M, q, τ) *array (*τ*-design)* C *exists in* $H(n, q)$, *i.e. evaluate*

$$\mathcal{L}(n, M; \tau; h) := \min\{\mathcal{E}(n, C; h) \ : \ |C| = M, \ C \subset H(n, q) \ e \ \tau\text{-}design\}.$$

Problem 4.0.4 *Let the potential function* h, *the length of the vectors* n, *the strength* τ *and the cardinality* $|C| = M = \lambda q^{\tau}$ *be fixed. Find the maximum possible energy* $\mathcal{U}(n, M; \tau; h)$, *such that an orthogonal* (n, M, q, τ) *array (*τ*-design)* C *exists in* $H(n, q)$, *i.e. evaluate*

$$\mathcal{U}(n, M; \tau; h) := \max\{\mathcal{E}(n, C; h) \ : \ |C| = M, \ C \subset H(n, q) \ e \ \tau\text{-}design\}.$$

We use combinatorial techniques to evaluate the problems outlined above. For this purpose, it is necessary to introduce the following definition.

Definition 4.1.1 *Let $C \subset H(n,q)$ be an (n, M, q, τ) orthogonal array and $x \in C$ be a point in C such that with respect to x the array C has distance distribution $P(x) = (p_0(x), p_1(x), \ldots, p_n(x))$. We call the energy of the distance distribution $P(x)$ of the orthogonal array C with respect to its internal point x the value of the following expression*

$$\mathcal{E}(x, C; h) := \frac{1}{|C|} \sum_{i=1}^{n} p_i(x) h(t_i),$$

where $t_i = 1 - \frac{2i}{n}$, i.e. t_i runs the set T_n of inner products in $H(n,q)$. This energy may be referred as the energy of the point $x \in C$.

Let $C = (n, M, q, \tau)$ be an orthogonal array in $H(n,q)$, and let $P_1(x_1)$, $P_2(x_2)$, ..., $P_s(x_s)$ be all the distinct distance distributions of C with respect to all the internal point for C appearing $k_1, k_2, \ldots, k_s$ times, respectively. We introduce the following theorem.

Theorem 4.1.2 *Let C be a (n, M, q, τ) orthogonal array in $H(n,q)$. Let $P_1(x_1)$, $P_2(x_2)$, ..., $P_s(x_s)$ be all the distinct distance distributions of points of C, appearing $k_1, k_2, \ldots, k_s$ times, respectively. Then the energy of C is*

$$\mathcal{E}(n, C; h) = \sum_{i=1}^{s} k_i \mathcal{E}(x_i, C; h).$$

In other words, we have

$$\mathcal{E}(n, C; h) \in \mathcal{E}(M) := \Big\{ \sum_{k_1+k_2+\cdots+k_s=M} k_i \mathcal{E}(x_i, C; h) \Big\}.$$

Let the set of all the possible distance distribution with respect to an internal point be $P(n, M, \tau) = \{P_1(x_1), P_2(x_2), \ldots, P_s(x_s)\}$. We denote the minimal and the maximal energy of a point of this set by

$$p = \min\{E(x_i, C; h) \ : \ s = 1, 2, \ldots, s\}$$

and

$$P = \max\{E(x_i, C; h) \ : \ s = 1, 2, \ldots, s\},$$

respectively

We are now in a position to state the general form of our combinatorial bounds on the energy of the τ-designs of M points in $H(n,q)$.

Theorem 4.2.1 *Let p and P be the minimum and maximum, respectively, of the possible energies of a distance distribution of an orthogonal array (τ-design) $C \subset H(n,q)$. Then*

$$Mp \leq \mathcal{L}(n, M, \tau; h) \leq \mathcal{U}(n, M, \tau; h) \leq MP.$$

An important corollary of this theorem is the special case when the orthogonal array C has an unique distance distribution. In this case we can calculate the exact energy of the array C.

Corollary 4.2.3 *Let the parameters q, n, M and τ be such that every (n, M, q, τ) orthogonal array in $\mathbb{H}(n, q)$ has the same (unique) distance distribution $P = P(x)$, $x \in C$ with respect to all of its points. Then for every potential function h these designs have optimal energy*

$$\mathcal{E}(n, C; h) = \mathcal{L}(n, M, \tau; h) = \mathcal{U}(n, M, \tau; h) = M\mathcal{E}(x, C; h).$$

Most applications [20, 10] require special types of potentials (mainly absolute monotonicity of h on $[-1, 1)$). In contrast, our bounds are valid for all potential functions h.

The Universal bound for the energy of an orthogonal array is outlined in [12]. A comparison between the two bounds is presented. The combinatorial bounds are better in some cases.

The fourth chapter is based on the following publication [18].

All calculations and algorithms, made for the purposes of this thesis, are realised in Maple. The current results can be found on the following web address [59] and the code will be provided upon request.

Scientific contributions

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

1. An algorithm (Algorithm 1) which reduces the set of distance distributions with respect to the internal points $P(n, M, 2, \tau)$ of a binary $(n, M, 2, \tau)$ orthogonal array was developed.

2. An algorithm (Algorithm 2 - main algorithm) which reduces the set of distance distributions with respect to an arbitrary point $W(n, M, 2, \tau)$ of a binary $(n, M, 2, \tau)$ orthogonal array was developed.

3. An algorithm (Algorithm 3) which reduces the set of distance distributions with respect to an arbitrary point $W(n, M, 2, \tau)$ of a binary $(n, M, 2, \tau)$ orthogonal array by removing two columns was developed.

4. The exact value of the minimum possible index of an orthogonal array has been found for the following parameters

$$\Lambda(9, 4, 2) = \Lambda(10, 4, 2) = \Lambda(11, 4, 2) = \Lambda(12, 4, 2) = 8$$

$$\Lambda(10, 5, 2) = \Lambda(11, 5, 2) = \Lambda(12, 5, 2) = \Lambda(13, 5, 2) = 8.$$

5. An algorithm (Algorithm 5) which reduces the set of distance distributions with respect to an arbitrary point $W(n, M, 3, \tau)$ of a ternary $(n, M, 3, \tau)$ orthogonal array was developed.

6. An algorithm (Algorithm 6) which reduces the set of distance distributions with respect to the internal points $P(n, M, 3, \tau)$ of a ternary $(n, M, 3, \tau)$ orthogonal array was developed.

7. The lower bound for the minimal index of an orthogonal $(17, 108, 3, 3)$ array has been improved, i.e. it is proved that $\Lambda(17, 3, 3) \geq 5$.

8. An algorithm (Algorithm 7) for obtaining bounds on the energy of orthogonal arrays for a fixed potential was developed.

9. The following combinatorial bounds for the value of the energy of an orthogonal array has been found

$$Mp \leq L(n, M, \tau; h) \leq U(n, M, \tau; h) \leq MP.$$

Approbation of the results

The results which are outlined in this paper have been published in the following 6 articles:

[16] Boyvalenkov P., Kulina H., Marinova T., Stoyanova M., Nonexistence of binary orthogonal arrays via their distance distributions, *Problems of Information Transmission*, Vol. 51(4), pages: 326–334 (2015), (Original Russian Text Published in Problemy Peredachi Informatsii, Vol. 51(4), pages: 23–31 (2015), ISSN: 0555-2923), Print ISSN: 0032-9460, Online ISSN: 1608-3253, https://doi.org/10.1134/S003294601504002X, Ref Web of Science, Impact Factor: 0.632 (2015), Quartile: Q_3 (2015).

[18] Peter Boyvalenkov, Tanya Marinova, Maya Stoyanova, Mila Sukalinska, Distance distributions and energy of designs in Hamming spaces, *Serdica Journal of Computing*, Vol. 9, No. 2, pages: 139–150 (2015), ISSN: 1314-7897 (Online), ISSN: 1312-6555 (Print), Ref zbMATH (Zbl 1387.94112).

[17] Peter Boyvalenkov, Tanya Marinova, Maya Stoyanova, Nonexistence of a few binary orthogonal arrays, *Discrete Applied Mathematics*, Vol. 217(2), pages: 144–150 (2017), ISSN: 0166-218X, https://doi.org/10.1016/j.dam.2016.07.023, Ref Web of Science, Impact Factor: 0.932 (2017), Quartile: Q_3 (2017).

[43] Tanya Marinova, Maya Stoyanova, Nonexistence of $(9, 112, 4)$ and $(10, 224, 5)$ binary orthogonal arrays, *Electronic Notes in Discrete Mathematics (containing the Proceedings of ACCT XV)*, Vol. 57, pages: 153-159 (March 2017), ISSN: 1571-0653, Ref Scopus, SJR: 0.262 (2017), SNIP 0.401 (2017), http://doi.org/10.1016/j.endm.2017.02.026.

[7] Boumova S., Marinova T., Ramaj T., Stoyanova M., Nonexistence of (17, 108, 3) ternary orthogonal array, *Ann. Sofia Univ., Fac. Math and Inf.*, Vol. 106, pages: 117-126 (2019), ISSN: 1313-9215 (print), ISSN: 2603-5529 (online), Ref MathSciNet (MR4125835).

[6] Boumova S., Marinova T., Stoyanova M., On ternary orthogonal arrays, *Proceedings Sixteenth International Workshop on Algebraic and Combinatorial Coding Theory*, ACCT XVI, September 2-9, 2018, Svetlogorsk (Kaliningrad region), Russia, pages: 102-105 (2018).

The results from articles [17] and [43] have been announced at the XV International Workshop on Algebraic and Combinatorial Coding Theory, ACCT–15, June 18-24, 2016, Albena, Bulgaria.

Two of the publications ([16],[17]) have Impact factor, one has SJR ([43]), and two are refereed in the scientific data bases - ZbMath and MathSciNet ([18], [7]).

The publications have been cited a total of 12 times, of which 10 are in Web of Science or Scopus.

Assoc. Prof. Maya Stoyanova, Ph.D. is a co-author of all of the articles. Furthermore, Prof. Peter Boyvalenkov, Doctor of Sciences, is a co-author of articles [16], [17] and [18]. Assoc. Prof. Silvia Boumova, Ph.D. is a co-author of papers [6] and [7]. Tedis Ramaj is

a co-author of the latter one. Assoc. Prof. Hristina Kulina, Ph.D., and Mila Sukalinska are co-authors of papers [16] and [18], respectively.

The results in this thesis were presented at the following national and international forums:

- Jubilee Conference: 125 years of Mathematics and Natural Sciences at Sofia University "St. Kliment Ohridski", Sofia, December 2014,
- National Coding Theory workshop with international participation "Professor Stefan Dodunekov", Veliko Tarnovo, November 2014,
- National Coding Theory workshop with international participation "Professor Stefan Dodunekov", village of Chiflika, November 2015,
- Spring Scientific Session of FMI-SU, "Algebra, Geometry, and Topology" Department, Sofia, March 2015,
- Spring Scientific Session of FMI-SU, "Algebra, Geometry, and Topology" Department, Sofia, March 2016,
- Seminar of "Mathematical Foundations of Informatics" Department, IMI-BAS, Sofia, December 2015,
- Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT-15, Albena, June 2016,
- National Coding Theory workshop with international participation "Professor Stefan Dodunekov", village of Chiflika, November 2019.

Acknowledgements

I would like to give my sincerest gratitude to my scientific advisor Assoc. Prof. Maya Stoyanova, Ph.D. for her invaluable advice and guidance. Furthermore, I would like to thank Prof. Peter Boyvalenkov, Doctor of Sciences, for the vast amount of knowledge he shared with me. Moreover, I would like to thank all of my co-authors - Assoc. Prof. Silvia Boumova, Ph.D., Assoc. Prof. Hristina Kulina, Ph.D., Tedis Ramaj, and Mila Sukalinska for providing me with different ideas and the opportunity to experience working within a team of scientists.

I would like to further thank all my colleagues from the Department of Algebra for believing in me.

Last but not least, I would like to thank my husband for his unconditional help and support.

Declaration of the authenticity of the presented results

I declare that the presented Ph.D. thesis contains original results, obtained from research conducted by myself (with the help and guidance of my scientific advisor and co-authors). The results obtained by other scientists have been thoroughly and clearly cited in the bibliography.

Signature:

Bibliography

[1] Abramowitz M., Stegun I.A., Handbook of Mathematical Functions, with Formulas, Graphs, and Mathematical Tables, *National Bureau of Standards*, Applied Mathematics Series, Vol. 55 (1964).

[2] Angelopoulos P., Evangalaras H., Koukouvinos C.,Lappas E., An effective step-down algorithm for the construction and the identification of non-isomorphic orthogonal arrays, *Metrika*, Vol. 66 (2), 139-149 (2007).

[3] Alon N., Goldreich O., Hastad J., Peralta R., Simple construction of almost k-wise independent random variables, *Random Struct. Algor.*, Vol. 3, 289-304 (1992).

[4] Bierbrauer J., Gopalakrishan K., Stinson D. R., Bounds for resilient functions and orthogonal arrays, *Lecture Notes in Computer Sciences*, Vol. 839, 247-256 (1994).

[5] Bierbrauer J., Gopalakrishan K., Stinson D. R., Orthogonal arrays, resilient functions, error-correcting codes and linear programming bounds, *SIAM J. Discrete Math.*, Vol. 9, 424-452 (1996).

[6] Boumova S., Marinova T., Stoyanova M., On ternary orthogonal arrays, *Proc. Sixteenth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT–16*, September 2-9, 2018, Svetlogorsk (Kaliningrad region), Russia, 102-105 (2018).

[7] Boumova S., Marinova T., Ramaj T., Stoyanova M., Nonexistence of $(17, 108, 3)$ ternary orthogonal array, *Ann. Sofia Univ., Fac. Math and Inf.*, Vol. 106, 117-126 (2019).

[8] Boumova S., Ramaj T., Stoyanova M., Computing distance distributions of ternary orthogonal arrays, *Compt. rend. Acad. bulg. Sci.*, 2020, accepted.

[9] Boyvalenkov P., Computing distance distributions of spherical designs, *Linear Algebra and Its Applications*, Vol. 226/228, 277-286 (1995).

[10] P. G. Boyvalenkov, P. D. Dragnev, D. P. Hardin, E. B. Saff, M. M. Stoyanova, Energy bounds for codes and designs in Hamming spaces, *Designs, Codes and Cryptography*, Vol. 82, Issue I, pp. 411–433 (2017).

[11] P. Boyvalenkov, D. Danev, On linear programming bounds for codes in polynomial metric spaces, *Problems of Information Transmission*, Vol. 34, No. 2, pp. 108-120 (1998).

[12] Peter Boyvalenkov, Danyo Danev, Maya Stoyanova, Refinements of Levenshtein bounds in q-ary Hamming spaces, *Problems of Information Transmission*, Vol. 54, No. 4, pp. 329–342 (2018).

[13] Boyvalenkov P., Kulina H., Computing distance distributions of orthogonal arrays, *Proc. Intern. Workshop ACCT2010*, Novosibirsk, Sept., 82-85 (2010).

[14] Boyvalenkov P., Kulina H., Investigation of binary orthogonal arrays via their distance distributions, *Problems of Information Transmission*, Vol. 49(4), 320-330 (2013). (Original Russian text: Problemy Peredachi Informatsii, Vol. 49, No. 4, 28–40, 2013).

[15] Boyvalenkov P., Kulina H., Stoyanova M., Nonexistence of certain binary orthogonal arrays, *Proc. 7th Intern. Workshop on Optimal Codes and Related Topics*, Sep. 6-12, 2013, Albena, Bulgaria, 65-70 (2013).

[16] Boyvalenkov P., Kulina H., Marinova T., Stoyanova M., Nonexistence of binary orthogonal arrays via their distance distributions, *Problems of Information Transmission*, Vol. 51(4), 326-334 (2015).

[17] Boyvalenkov P., Marinova T., Stoyanova M., Nonexistence of a few binary orthogonal arrays, *Discrete Applied Mathematics*, Vol. 217(2), 144-150 (2017).

[18] Peter Boyvalenkov, Tanya Marinova, Maya Stoyanova, Mila Sukalinska, Distance distributions and energy of designs in Hamming spaces, *Serdica Journal of Computing*, Vol. 9, No. 2, 139–150 (2015).

[19] Bulutoglu D.A., Margot F., Classification of orthogonal arrays by integer programming, *Jornal of Statistical Planning and Inference*, Vol. 138, 654-666 (2008).

[20] Cohn H., Zhao Y., Energy-minimizing error-correcting codes, *IEEE Transactions on Information Theory*, Vol. 60, 7442-7450. (2014).

[21] Delsarte P., An Algebraic Approach to the Association Schemes in Coding Theory, *Philips Res. Rep. Suppl.*, Vol. 10, 1973.

[22] Delsarte P., Four fundamental parameters of a code and their combinatorial signficance, *Information and Control*, Vol. 23, 407-438 (1973).

[23] Delsarte P., Levenshtein L.I., Association schemes and coding theory, *IEEE Transactions on Information Theory*, Vol. 44, 2477-2504 (1998).

[24] Delsarte P., Bounds for Unrestricted Codes by Linear Programming, *Philips Research Reports*, Vol. 27, 272-289 (1972).

[25] Dunkl C.F., Discrete quadrature and bounds on t-designs, *Michigan Math. J.*, Vol. 26, 81-102 (1979).

[26] Fazekas G., Lenvestein V.I., On Upper Bounds for Code Distance and Covering Radius of Designs in Polynomial Metric Spaces, *Journal of combinatorial theory*, Series A, Vol. 70, 267-288 (1995).

[27] Hamming, R. W., Error detecting and error correcting codes, *Bell System Technical Journal*, Vol. 29, 147–160 (1950).

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

[29] Helleseth T., Kløve T., Lenvestein V.I., A bound for codes with given minimum and maximum distances,' *IEEE International Symposium on Information Theory* Seattle, USA, 292–296 (2006).

[30] Jackson W. A., Martin K., A combinatorial interpretation of ramp schemes, *Australasian Journal of Combinatorics*, Vol. 14, 51–60 (1996).

[31] Petteri Kaski, Patric R.J. Östergård, Classification Algorithms for Codes and Designs, *Springer Verlag*, Berlin Heidelberg (2006).

[32] Khalyavin A. V., Estimates of the capacity of orthogonal arrays of large strength, *Moscow Univ. Math. Bull.*, Vol. 65, 130-131 (2010).

[33] Kleinberg, Jon; Tardos, Éva, Algorithm Design (2nd ed.), *Addison-Wesley*, ISBN 0-321-37291-3 (2006).

[34] I.Krasikov, S.Litsyn, On integral zeros of Krawtchouk polynomials, Journal of Combinatorial Theory, *Ser. A*, 74(1), 71-99 (1996).

[35] I.Krasikov, S.Litsyn, Linear programming bounds for codes of small codes, *Europ. J. Comb.*, Vol.18, 647-656 (1997).

[36] Kurosawa K., Johannsson T., Stinson D. R., Almost k-wise independent sample spaces and their cryptologic applications, *Journal of Cryptology*, Vol. 14, 231–253 (2001).

[37] Levenshtein V.I., Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces, *IEEE Transactions on Information Theory*, Vol. 41, 1303-1321 (1995).

[38] Levenshtein V.I., Universal bounds for codes and designs, *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds., Elsevier, Amsterdam, Ch. 6, 499-648 (1998).

[39] Levenshtein V.I., Designs as maximum codes in polynomial metric spaces, *Acta Applicandae Mathematica*, Vol. 29, 1-82 (1992).

[40] Levenshtein V.I., Bounds for packings in metric spaces and certain applications, *Probl. Kibern.*, Vol. 40, 44-110 (1983) (in Russian).

[41] MacWilliams F. J. , Sloane N. J. A., The Theory of Error-Correcring Codes, Amsterdam, The Netherlands: North Holland, 1977.

[42] Manev, N. L., On the distance distributions of Orthogonal Arrays, *Problems of Information Transmission*, Vol. 56, 45–55 (2020).

[43] Marinova T., Stoyanova M., Nonexistence of $(9, 112, 4)$ and $(10, 224, 5)$ binary orthogonal arrays, *Electronic Notes in Discrete Mathematics*, containing the Proceedings of ACCT XV, Vol. 57, 153–159 (2017).

[44] Nikiforov A. F., Suslov S. K., Uvarov V. B. , Classical Orthogonal Polynomials of a Discrete Variable *Springer Series in Computational Physics*, Berlin: Springer-Verlag (1991).

[45] Ostergard P.R.J., Baicheva T., Kolev E., Optimal binary one-error-correcting codes of length 10 have 72 codewords, *IEEE Transactions on Information Theory*, Vol. 45, 1229-1231 (1999).

[46] A. Perttula, Bounds for binary and nonbinary codes slightly outside of the Plotkin range, *Tampere University of Technology Publ.*, 14 (1982).

[47] Plotkin M., Binary codes with specified minimum distance, *IRE Transactions on Information Theory*, Vol. 6, 445–450 (1960).

[48] Raghavarao D., Constructions and Combinatorial Problems in Design of Experiments, New York : Wiley, 1971.

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

[50] A. Samorodnitsky, On the optimum of Delsarte's linear program, *J. Combin. Theory*, Ser. A 96, 261-287 (2001).

[51] Schoen E. D., Eendebak P. T., Nguyen M. V. M., Complete enumeration of pure-level and mixed-level orthogonal arrays, *Journal of Combinatorial Designs*, Vol. 18, 123-140 (2009).

[52] Seiden E., Zemach R., On orthogonal arrays, *Ann. Math. Statist.*, Vol. 37, 1355-1370 (1996).

[53] Singleton R. C., Maximum distance q-ary codes, *IEEE Transactions on Information Theory*, Vol. 10, 116-118 (1964).

[54] J. Stuffken, B. Tang, Complete enumeration of two-level orthogonal arrays of strength d, *The Annals of Statistics*, Vol. 35, 793–814 (2007).

[55] Szegő G., *Orthogonal Polynomials*, American Mathematical Society Colloquium Publications 23, Providence, RI, 1939.

[56] Taguchi, G., System of Experimental Design: Engineering Methods to Optimize Quality and Minimize Costs, *UNIPUB/Kraus International Publications*, 1987.

[57] Vaudenay S., Decorrelation: A theory for block cipher security, *Journal of Cryptology*, Vol. 16, 249–286 (2003).

[58] http://neilsloane.com/oadir/index.html

[59] https://store.fmi.uni-sofia.bg/fmi/algebra/mstoyanova.shtml