Доклади на Българската академия на науките
Comptes rendus de l'Académie bulgare des Sciences

Tome 74, No 2, 2021

MATHEMATICS

Combinatorics

COMPUTING DISTANCE DISTRIBUTIONS OF TERNARY ORTHOGONAL ARRAYS

Silvia Boumova*,, Tedis Ramaj*, Maya Stoyanova***

(*Submitted by Academician V. Drensky on November 16, 2020*)

Abstract

Orthogonal Arrays (OA) play important roles in statistics (used in designing experiments), computer science and cryptography. The most important problems are those about their existence and classification of non-isomorphic classes of OA with given parameters. The solving of these problems requires possible Hamming distance distributions of studied orthogonal array to be determined. In this paper we propose a method for computing of distance distributions of OA with given parameters. Comparing computed possible distance distributions of the considered OA with ones of its derivative OAs we proved some nonexistence results and found some restrictions over structure of the studied OA.

Key words: Hamming space, Orthogonal Arrays, Krawtchouk polynomials, distance distributions

2020 Mathematics Subject Classification: 05B15, 15B36

1. Introduction. Orthogonal arrays were introduced by Rao (1946) and since then have been studied by many researchers from various fields, both from theoretical and practical point of view (see [1]). The latest results and achievements can be found on the web sites [2, 3].

The research of the first author was partially supported by Grant KP-06N32/1-2019 of the Bulgarian National Science Fund. The research of the second author was partially supported by the Science Foundation of Sofia University under contract 80-10-151/24.04.2020. The research of the third author was partially supported by Grant KP-06-N32/2-2019 of the Bulgarian National Science Fund.

DOI:10.7546/CRABS.2021.02.03

Definition 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).

The parameter $\lambda = M/q^t$ is called *index*. In what follows we assume that $\mathcal{A}$ is the ring $\mathbb{Z}_q$ of integers modulo q or the finite field $GF(q)$ of q elements although some properties hold even for $\mathcal{A}$ commutative ring with unity. *Hamming distance* $d(\mathbf{x}, \mathbf{y})$ between two vectors $\mathbf{x}$ and $\mathbf{y}$ of $\mathcal{A}^n$ is the number of places in which they differ:

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

Hamming weight $\mathrm{wt}(\mathbf{c})$ of a vector $\mathbf{c} \in \mathcal{A}^n$ is the number of its nonzero entries. Clearly $\mathrm{wt}(\mathbf{c}) = d(\mathbf{c}, \boldsymbol{o})$, where $\boldsymbol{o}$ is all zero vector.

Let C be a subset (in general multi subset) of $\mathcal{A}^n$ and $\mathbf{x} \in \mathcal{A}^n$ be a fixed vector. The set of nonnegative 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* $\mathbf{x}$.

It should be emphasized that knowledge of distance distribution of C with respect to points of $\mathcal{A}^n$ is of great importance for studying codes and orthogonal arrays. In [4–6] authors compute $\mathbf{p}(\mathbf{x})$ as a nonnegative integer solution of a linear system with matrix (t_j^i), where $t_j = 1 - \frac{2j}{n}$, $j = 0, \ldots, n$ ([7]). They received the possible values of $\mathbf{p}(\mathbf{x})$ and use them to prove the nonexistence of orthogonal arrays with given parameters.

The information that can be derived from aforesaid linear system with rational coefficients is not too much. All $(M+1)^{n+1}$ possible nonnegative integer $(n+1)$-tuples have to be tested if they satisfy the system.

In [8] the author shows how to obtain many linear systems with integer coefficients that $\mathbf{p}(\mathbf{x})$ satisfies. This approach enables upper bounds for all p_i to be obtained that significantly reduce the number of potential candidates for $\mathbf{p}(\mathbf{x})$. It also makes possible to avoid testing whether given vector is a solution of the system and to replace this test with checking only the signs of $t+1$ coordinates of that vector.

The next section presents the necessary notions and results for orthogonal arrays. In Section 3 we describe the algorithm given in [8]. Section 4 presents our approach to find expressions for some parameters that can give bounds for possible distance distributions. In the last section the obtained results about orthogonal arrays are presented.

2. Preliminaries. The KRAWTCHOUK polynomials (see, e.g., [7,9–11]) are well known and we list only their properties that we need. Let $\mathbb{R}^{n+1}[x]$ be the linear space of polynomials of degree up to n over real numbers $\mathbb{R}$. Let $q \geq 2$ be

an integer. The bilinear map defined by

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

satisfies the axioms for scalar product.

Definition 2. *Krawtchouk polynomial* is a polynomial defined by

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

The Krawtchouk polynomial $K_k(x;\, n, q)$ is a polynomial of degree k in x with leading coefficient $(-q)^k/k!$. The parameters q and n have already been fixed, so we omit n and q and write only $K_k(x)$.

Corollary 2.1. *For fixed q and n the Krawtchouk polynomials $K_0(x)$, $K_1(x)$, ..., $K_n(x)$ satisfy*

1) *First orthogonality relation*

$$\langle K_k, K_l\rangle = \frac{1}{q^n}\sum_{i=0}^{n}\binom{n}{i}(q-1)^i K_k(i)K_l(i) = \binom{n}{k}(q-1)^k\,\delta_{kl}; \tag{2}$$

2) *Second orthogonality relation*

$$\sum_{i=0}^{n} K_k(i)K_i(l) = q^n\delta_{kl}. \tag{3}$$

From (2) they are an *orthogonal basis* of $\mathbb{R}^{n+1}[x]$ according to scalar product (1). And second orthogonality relation follows from relation

$$(q-1)^i\binom{n}{i}K_k(i) = (q-1)^k\binom{n}{k}K_i(k). \tag{4}$$

The next theorem is a consequence from the fact that $K_0(x)$, $K_1(x)$, ..., $K_n(x)$ form an orthogonal basis of $\mathbb{R}^{n+1}[x]$.

Theorem 2.2. *For any polynomial $f(x) \in \mathbb{R}^{n+1}[x]$ there is a unique expansion*

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

where

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

Indeed $f_k = \langle f(x), K_k(x)\rangle / \langle K_k(x), K_k(x)\rangle$. The second equality follows from (4).

Following [1] some properties of OA's will be showed.

Theorem 2.3 ([1]). *For an $OA(M, n, q, t)$ the following properties hold*:

(i) *A permutation of the rows or columns in $OA(M, n, q, t)$ results in orthogonal array with the same parameters.*

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

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

(iv) *If $\mathbf{A} = \begin{pmatrix} \mathbf{A}_1 \\ \mathbf{A}_2 \end{pmatrix}$ is an $OA(M, n, q, t)$, where $\mathbf{A}_1$ itself is an $OA(M_1, n, q, t_1)$, then $\mathbf{A}_2$ is an $OA(M - M_1, n, q, t_2)$ with $t_2 \geq \min\{t, t_1\}$.*

Recall that herein the alphabet $\mathcal{A}$ is the ring $\mathbb{Z}_q$ of integers modulo q or the finite field $GF(q)$ of q elements. The next two results are due to DELSARTE [12–14].

Lemma 2.4. *Let C be $OA(M, n, q, t)$ and $\mathbf{x} \in \mathcal{A}^n$. If $\mathbf{p}(\mathbf{x}) = (p_0, p_1, \ldots, p_n)$ is the distance distribution of C with respect to $\mathbf{x}$, then*

$$\sum_{i=0}^{n} p_i K_k(i) = 0 \quad \text{for} \quad k = 1, \ldots, t. \tag{5}$$

Let C be a (multi-)subset of $\mathcal{A}^n$. The sequence of rational numbers $\{A_i\}$, $i = 0, 1, \ldots, n$, defined by

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

is called *distance distribution* of C. Obviously $\{A_i\}$ is the mean of $\mathbf{p}(\mathbf{x})$ on $\mathbf{x} \in C$.

Lemma 2.5. *Let C be $OA(M, n, q, t)$ and $\{A_i\}$, $i = 0, 1, \ldots, n$ be distance distribution of C. Then*

$$\sum_{i=0}^{n} A_i K_k(i) \geq 0 \quad \text{for any} \quad k = 0, 1, \ldots, n.$$

3. Algorithm for effectively computing distance distributions. BOYVALENKOV et al. [4–6] 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 Vandermonde matrix (t_j^i), where $t_j = 1 - \frac{2j}{n}$, $j = 0, \ldots, n$.

Recently, MANEV [8] using properties of Krawtchouk polynomials showed different representations of this system. Some of these can facilitate fast computation of distance distributions. Manev's results are summarized in Theorem 3.2. In this section we follow the results of [8].

Theorem 3.1. *Let C be $OA(M,n,q,t)$ 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 any polynomial $f(x)$ of degree $\deg f\le t$ the following hold*

$$(6)\qquad \sum_{i=0}^{n} p_i f(i) = f_0 M, \quad f_0 = \frac{1}{q^n}\sum_{i=0}^{n} f(i)K_i(0) = \frac{1}{q^n}\sum_{i=0}^{n}\binom{n}{i}(q-1)^i f(i),$$

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

Theorem 3.2 ([8])**.** *Let C be $OA(M,n,q,t)$ 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 $k=0,1,\ldots,t$ the following systems hold*:

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

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

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

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

One can choose suitable polynomials in Theorem 3.1 to prove Theorem 3.2.

The following theorems are important and basic in more efficient algorithm for computing distance distribution $\mathbf{p}=\mathbf{p}(\mathbf{v})$ which is described below.

Theorem 3.3 ([8])**.** *Let $\mathbf{A}=(a_{ki})=(i^k)$, $k=0,1,\ldots,t$, $i=1,2,\ldots,n$. For $t<m\le n$ 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.

Lemma 3.4. *Let $\mathbf{R}_t=(r_{ij})=\left(\binom{j}{i}\right)$, where $i,j=0,1,2,\ldots,t$. Its inverse matrix is*

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

ALGORITHM [8]

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 $\mathbf{u}$ has maximal values. Compute a partial solution from Theorem 3.2 (iv) putting zeros in all positions but in the chosen $t+1$ positions.

P3. Apply the **Null Space Algorithm**.

NS 1. Construct the matrix $\mathbf{A}_s = (a_{kl}) = \left(\binom{l-s}{k}\right)$. It contains the matrix $\mathbf{R}_t$ defined in Lemma 3.4 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 3.4) 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

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

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

NS 4. Generate all linear combinations of the rows of $\mathbf{G}$ 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 3.2 (iv).

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

Solutions with zero first coordinate are distance distribution with respect to an external point for the orthogonal array while ones with nonzero first coordinate correspond to distributions with respect to internal point. If the first coordinate is greater than 1 it means that the point appears more than once, i.e., the orthogonal array is a multi-set.

4. Our approach. Minimization of the upper bound $\mathbf{u}$ is very important. Decreasing even by 1 in one position of $\mathbf{u}$ leads to significant decreasing of numbers of checks. That is why our efforts are directed to understand the structure of matrix $\mathbf{B}$ and to make some better bounds for $\mathbf{u}$.

Let us consider system (iv) in Theorem 3.2 in details.

$$A_s p^t = a, \tag{7}$$

where

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

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

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

where $k = 0, \dots, t$. Columns of A corresponding to $l = s, \dots, s+t$ form $(t+1)\times(t+1)$ matrix $R_t = (r_{ij}) = \left(\binom{j}{i}\right)$. Multiplying system (7) by R_t^{-1} we get $Bp^\tau = b$, where $B = R_t^{-1}A = (b_{ml})$ and $b = (b_0, \dots, b_t)^\tau$, that is,

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

and

$$b_m = (-1)^m\lambda q^{t-n}\sum_{i=0}^{n}\left(\binom{n}{i}(q-1)^i\sum_{j=0}^{t}\binom{j}{m}\binom{i-s}{j}\right), \quad m = 0, 1, \dots, t. \tag{8}$$

To find good expression for elements b_{ml} from matrix B we use the following lemma.

Lemma 4.1. *The following hold:*

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

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

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

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

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

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

Based on Lemma 4.1 we can evaluate the elements of the matrix B by the next theorem. The received analytical expression of the matrix B helps a lot in faster calculation of distance distributions and finding analytical bounds for covering radius [15] and minimal distance of orthogonal arrays.

Theorem 4.2. *The following hold*:

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

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

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 $l = s, s+1, \ldots, s+t$.

Now we can simplify expression for b_m. Applying Lemma 4.1 to (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

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

Thus the received formulae 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 4.3. *The numbers b_{ml} have 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 4.2 (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 4.4. *For t even number the inequality holds*

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

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

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

5. Relation between distance distributions of OA(M,n,q,t) and its derivative OAs. The information of possible distance distributions of an orthogonal array with respect to any point could be used to solve existence and classification problems. It provides useful information about the covering radius of the orthogonal array considered as a q-ary code in the Hamming space.

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 $\check{C}$ 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 Theorem 2.3

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

Using the described algorithm we compute all possible distance distributions of C, C_i, $\check{C}$ as well as ones of any other necessary array 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 $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ *dominates* another vector $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ if $a_i \geq b_i$ for all $i = 1, \ldots, n$.

Corollary 5.1. *If vector $p = (p_0, p_1, \ldots, p_n)$ is 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* $p_0^0 \geq 1$;

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

(i) *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;

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

We will call $\check{\mathbf{p}}$, $\overline{\mathbf{p}}$, $\mathbf{p}^0$ *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 $\check{\mathbf{p}}$, $\overline{\mathbf{p}}$, $\mathbf{p}^0$. The following result holds.

Theorem 5.2 ([4, 8])**.** *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*

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

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. □

6. Results.

Theorem 6.1. *The minimal index for ternary arrays with strength $t = 3$ and length 17 and 16 is $\lambda = 5$.*

Proof. We have to prove that an $OA(108, 17, 3, 3)$ and an $OA(108, 16, 3, 3)$ 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 the $OA(108, 17, 3, 3)$ and the $OA(108, 16, 3, 3)$ are 10 and 49, respectively.

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

3. Then we apply Corollary 5.1. Only nine vectors $\mathbf{p}$ of the $OA(108, 17, 3, 3)$ dominate internal distributions $\mathbf{p}^0$ of the $OA(36, 16, 3, 2)$.

4. For any pair $(\mathbf{p}, \mathbf{p}^0)$ we compute the difference $\overline{p} = (\overline{p}_0, \overline{p}_1, \ldots, \overline{p}_{n-1})$ (see Corollary 5.1). Then we test whether $\overline{p}$ is an external distribution for $C_1 \cup C_2$ that are the $OA(72, 16, 3, 2)$ and the $OA(72, 15, 3, 2)$ arrays, respectively. This means that the set of received distance distributions have to satisfy system of equations (Theorem 3.2).

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

6. The case $n = 16$ is more complicated. For seven of pairs $(\mathbf{p}, \mathbf{p}^0)$ the corresponding vectors $\overline{p}$ satisfy the system for the $OA(72, 15, 3, 2)$. Hence we have to apply Theorem 5.2 for the rest $\overline{p}$. No one passes this test. Therefore the $OA(108, 16, 3, 3)$ does not exist. □

Remark. The nonexistence result for an $OA(108, 17, 3, 3)$ has already been obtained using another method and appeared in [16].

Structural results

Structure of the $OA(108, 15, 3, 3)$

Applying the aforesaid approach we obtain four from 119 possible internal distance distributions for the $OA(108, 15, 3, 3)$ 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 constructing the $OA(108, 15, 3, 3)$ array.

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

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

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

is internal distribution for $\check{C}$.

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

REFERENCES

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

[2] Sloane N. J. A. http://neilsloane.com/oadir/index.html.

[3] A Library of Distance Distributions of Ternary Orthogonal Arrays, https://store.fmi.uni-sofia.bg/fmi/algebra/stoyanova/toa.html.

[4] Boyvalenkov P., H. Kulina (2013) Investigation of binary orthogonal arrays via their distance distributions, Probl. Inf. Transm., **49**(4), 320–330.

[5] Boyvalenkov P., T. Marinova, M. Stoyanova (2017) Nonexistence of a few binary orthogonal arrays, Discret. Appl. Math., **217**(2), 144–150.

[6] Boumova S., T. Marinova, M. Stoyanova (2018) On ternary orthogonal arrays. In: Proc. 16th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-XVI), Svetlogorsk, Russia, 2–8 September 2018, 102–105, https://www.dropbox.com/s/h7u89lh8vyirww9/Proceedings\%20final.pdf?dl=0.

[7] Levenshtein Vl. (1995) Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces, IEEE Trans. Inform. Theory, **41**(5), 1303–1321.

[8] Manev N. L. (2020) On the distance distributions of Orthogonal Arrays, Probl. Inf. Transm., **56**(1), 45–55.

[9] Krawtchouk M. (1929) Sur une généralisation des polynômes d'Hermite, Compt. Rend., **189**(17), 620–622.

[10] Szegő G. (1939) Orthogonal Polynomials, AMS Col. Publ., **23**, Providence, RI.

[11] MacWilliams F. J., N. J. A. Sloane (1977) The Theory of Error-Correcting Codes, North Holland, Amsterdam, The Netherlands.

[12] Delsarte Ph. (1972) Bounds for unrestricted codes by linear programming, Philips Res. Rep., **27**, 272–289.

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

[14] Delsarte Ph. (1973) An algebraic approach to the association schemes of coding theory, Philips Res. Rep. Suppl., No 10, 97 pp.

[15] Boumova S., T. Ramaj, M. Stoyanova (2020) On covering radius of orthogonal arrays. In: Proc. 17th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-XVII), Bulgaria, Oct. 11–17, 2020, online.

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

*Faculty of Mathematics and Informatics
Sofia University "St. Kliment Ohridski"
5, J. Bourchier Blvd
1164 Sofia, Bulgaria
e-mails: boumova@fmi.uni-sofia.bg
tramaj@fmi.uni-sofia.bg
stoyanova@fmi.uni-sofia.bg

**Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Akad. G. Bonchev St, Bl. 8
1113 Sofia, Bulgaria