Article

Bounds for the minimum distance and covering radius of orthogonal arrays via their distance distributions

Silvia Boumova [1], Peter Boyvalenkov [2]* and Maya Stoyanova [3]

[1] Faculty of Mathematics and Informatics, Sofia University, 5 James Bourchier Blvd., 1164 Sofia, Bulgaria; Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 8 G. Bonchev Str., 1113 Sofia, Bulgaria; boumova@fmi.uni-sofia.bg
[2] Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 8 G. Bonchev Str., 1113 Sofia, Bulgaria; peter@math.bas.bg
[3] Faculty of Mathematics and Informatics, Sofia University, 5 James Bourchier Blvd., 1164 Sofia, Bulgaria; stoyanova@fmi.uni-sofia.bg
* Correspondence: stoyanova@fmi.uni-sofia.bg (M. S.);

Abstract: We propose two methods for obtaining estimations on the minimum distance and covering radius of orthogonal arrays. Both methods are based on knowledge about the (feasible) sets of distance distributions of orthogonal arrays with given length, cardinality, factors and strength. New bounds are presented either in analytic form and as products of an ongoing project for computation and investigation of the possible distance distributions of orthogonal arrays with parameters in doable ranges.

Keywords: Orthogonal Arrays; Distance distributions; Minimum distance; Covering radius

1. Introduction

Orthogonal Arrays (OAs) have been studied for wide range of practical applications in the industry (planning experiments, parts testing, etc.), medicine (drug testing, clinical trials, etc.), agriculture and others, and also for their applications in computer science; among them software testing, big data, and data protection (because of strong relations to error-correcting codes [14]).

Strong cybersecurity relations come from the applications of OAs in the cryptography, such as these in authentification without secrecy [19,20] and constructions of secret sharing schemes [8,20], encryption schemes [15], and universal hash functions [7,13,21].

Let H_q be an alphabet of q letters and H_q^n be the Hamming space over H_q. Here q is not necessarily a prime power, i.e. we do not need any structure of the alphabet.

Definition 1.1. *An orthogonal array (OA) of strength t and index λ in H_q^n consists of the rows of an $M \times n$ matrix C with the property that every $M \times t$ submatrix of C contains all ordered t-tuples of H_q^t, each one exactly $\lambda = M/q^t$ times as rows. We denote C by $OA(M, n, q, t)$.*

Definition 1.1 shows that the main parameters of OAs are the cardinality M, the length n, the alphabet size q and the strength[1] t, and the index $\lambda = M/q^t$. The alphabet letters are also called levels, the rows of the OA are also known as runs and the columns are factors.

In this paper, we are interested in two further important parameters – the minimum distance and the covering radius of OAs. We examine these parameters via their relations to the set of distance distributions which can be computed for given M, n, q, and t as shown next.

[1] The strength is the maximal possible t.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 December 2021 doi:10.20944/preprints202112.0293.v1

Definition 1.2. *Let C be an $OA(M,n,t,q)$ and $x \in H_q^n$. The distance distribution of C with respect to x is the $(n+1)$-tuple*

$$w = w(x) = [w_0(x), w_1(x), \ldots, w_n(x)],$$

where $w_i(x) = |\{y \in C | d(x,y) = i\}|$, $i = 0, \ldots, n$, and $d(x,y)$ is the Hamming distance.

Repetition of rows in Definition 1.1 is allowed but we will consider mainly simple OAs, where each row appears only once. However, in the investigations of related (to an given OA) OAs, for example by deleting columns of the original OA, it will be possible to have multiple rows and we take this into account in our computations.

For given M, n, q, and t, the distance distributions can be computed as functions of the main parameters in various ways based on classical results of Delsarte [9,10] (see also [11,16]).

Theorem 1.3 (Delsarte [9,10])**.** *Let C be an $OA(M,n,q,t)$ and $x \in H_q^n$. If $w(x) = [w_0, w_1, \ldots, w_n]$ is the distance distribution of C with respect to x, then*

$$\sum_{i=0}^{n} w_i K_k^{(n,q)}(i) = 0, \quad k = 1, \ldots, t, \tag{1}$$

where

$$K_i^{(n,q)}(z) := \sum_{j=0}^{i} (-1)^j (q-1)^{i-j} \binom{z}{j} \binom{n-z}{i-j}, \quad i = 0, 1, \ldots, n,$$

are the Krawtchouk polynomials [22].

The Vandermonde-type system (1) from Theorem 1.3 has $t+1$ linear equations and $n+1$ unknowns. The set of its solutions is a subspace of $\mathbb{Q}^{n+1}$. Moreover, the admissible values of the elements of the solutions are only the integers from the set $\{0, 1, \ldots, q^n\}$. Therefore, there are finitely many possible solutions of the system (1), which can be found and further investigated. This idea was first applied in [4] and followed in [2,3,5,6,18] and others.

The paper is organized as follows. In Section 2 we describe the relations between the distance distributions and the minimum distance and covering radius of OAs. Theorem 2.1 explains out methodology for obtaining estimations for the targeted parameters. Section 3 is devoted to new bounds obtained by investigation of analytical expressions for suitably chosen distance distributions. In Section 4 we present an approach for derivation of new bounds (and exact values in some cases) based on knowledge of possible sets of distance distributions for given main parameters of OAs.

2. Distance distributions, minimum distance and covering radius of orthogonal arrays

We need to make difference between the distance distributions with respect to internal ($x \in C$) or external ($x \in H_q^n \setminus C$) points. It is easy to see that if $x \in C$, then $w_0(x) \geq 1$ (with an equality if and only if x is not repeated in C) and if $x \in H_q^n \setminus C$, then $w_0(x) = 0$. We denote by

$$P(C) := \{p = [p_0(x) \geq 1, p_1(x), \ldots, p_n(x)] : x \in C\}$$

the set of all distance distributions of C with respect to $x \in C$, calling the elements of $P(C)$ *internal* distance distributions, and, similarly, by

$$R(C) := \{r = [r_0(x) = 0, r_1(x), \ldots, r_n(x)] : x \in H_q^n \setminus C\}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 December 2021 doi:10.20944/preprints202112.0293.v1

the set of all distance distributions of C with respect to $x \notin C$, calling the elements of $R(C)$ *external* distance distributions. Thus, we use p and r to replace w in order to underline the difference between the internal (in $P(C)$) and external (in $R(C)$) distance distributions. It is clear that $W(C) = P(C) \cup R(C)$ is a disjoint union.

Switching to the existence/classification problem for OAs, in what follows we will consider the sets of distance distributions for given parameters M, n, q, and t instead of these of a particular OA. Thus, we will denote and consider the sets $P_f(M,n,q,t)$, $R_f(M,n,q,t)$, and $W_f(M,n,q,t)$, analogs of $P(C)$, $R(C)$, and $W(C)$, as the sets of all feasible distance distributions of (sometimes only putative) OA's having these parameters. The subscript f is set for "feasible" and means that the actual sets of any $OA(M,n,q,t)$ could be subsets, but not necessarily coinciding with $P_f(M,n,q,t)$, $R_f(M,n,q,t)$, and $W_f(M,n,q,t)$, respectively. The feasible sets of distance distributions can be further reduced by investigations of the relations between hypothetical $OA(M,n,q,t)$ and its related orthogonal arrays as shown in [4–6] and others.

For an orthogonal array C in H_q^n its minimum distance is

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

and its covering radius is

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

respectively. Given M, n, q, and t, we define the quantities

$$MinD(M,n,q,t) := \min\{d(C) : C \text{ is an } OA(M,n,q,t)\},$$

$$MaxD(M,n,q,t) := \max\{d(C) : C \text{ is an } OA(M,n,q,t)\},$$

and

$$CR(M,n,q,t) = \min\{\rho(C) : C \text{ is an } OA(M,n,q,t)\}.$$

Simple OAs are also (often very good) error-correcting codes. Thus, it makes sense to consider the quantities like $MaxD(M,n,q,t)$ and $CR(M,n,q,t)$ whose importance is well known from the coding theory. Since OAs are expected to be well distributed in the ambient space H_q^n, the investigation of $MinD(M,n,q,t)$ makes sense as well along with $CR(M,n,q,t)$.

Bounds for the minimum distance and covering radius of orthogonal arrays were considered earlier by many authors. Tietäväinen [23,24] was the first to investigate the relations between the covering radius and the strength. More references can be found in the paper [12] and the book [14]. However, it seems that systematic investigations of the relation between minimum distance and covering radius and knowledge about distance distributions, has not started so far. In our tutorial paper [1] we presented many examples and announced some of the bounds from this paper.

We next explain the basic relations between the distance distributions and the minimum distance and covering radius of OAs. It follows immediately from the definitions that if C is an OA with sets of distance distributions $P(C)$ and $R(C)$, then

$$d(C) = 1 + \min\{i : p_1(x) = \cdots = p_i(x) = 0\},$$

where the minimum is taken over $p \in P(C)$, and

$$\rho(C) = 1 + \max\{j : r_0(x) = r_1(x) = \cdots = r_j(x) = 0\},$$

where the maximum is taken over $r \in R(C)$, respectively. If the existence of C is undecided, or if there are many possible OAs with the same main parameters as C, the quantities in the right hand sides of the last two equalities serve as a lower bound for

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 December 2021 doi:10.20944/preprints202112.0293.v1

$d(C)$ and a upper bound for $\rho(C)$, respectively. More precisely, we have the following statement.

Theorem 2.1. *Let n, M, q, and t be feasible parameters for orthogonal arrays in H_q^n and let $P_f(M,n,q,t)$ and $R_f(M,n,q,t)$ be sets of feasible internal and external distance distributions of C, respectively. Then the following inequalities are valid:*

$$MinMD(M,n,q,t) \geq 1 + \min\{i : p_1(x) = \cdots = p_i(x) = 0\}, \tag{2}$$

$$MaxMD(M,n,q,t) \leq 1 + \max\{i : p_1(x) = \cdots = p_i(x) = 0\}, \tag{3}$$

where both the minimum and maximum are taken over all distributions $p \in P_f(M,n,q,t)$, and

$$CR(M,n,q,t) \leq 1 + \max\{j : r_0(x) = r_1(x) = \cdots = r_j(x) = 0\}, \tag{4}$$

where the maximum is taken over all distributions $r \in R_f(M,n,q,t)$.

Proof. Assume that $C \subset H_q^n$ is an $OA(M,n,q,t)$ and x and y are points of C at distance $d(C)$. Then $p_1(x) = \cdots = p_{d(C)-1}(x) = 0$ since there are no points of C at distance less than $d(C)$. This proves (2) and, since it is true also for all points $x \in C$ which do not have $y \in C$ at distance $d(C)$, proves (3) as well.

To prove (4) we consider a point $x \in H_q^n \setminus C$ at distance $\rho(C)$ to C. This means that $p_1(x) = \cdots = p_{\rho(C)-1}(x) = 0$, which proves (4). □

Assuming the existence of an $OA(M,n,q,t)$ we can apply Theorem 2.1 in two ways. First, we can derive and investigate analytical expressions for specific entries (close to the maximal possible number of initial zeros) of the distance distributions. Second, we can investigate current databases of feasible distance distributions (i.e. sets $P_f(M,n,q,t)$ and $R_f(M,n,q,t)$) to determine minimums and maximums in Theorem 2.1. We usually find some initial $P_f(M,n,q,t)$ and $R_f(M,n,q,t)$ as sets of all integer non-negative solutions of the system (1), possibly after some restrictions. In the next stages we apply the techniques from [4–6] in order to obtain reduced $P_f(M,n,q,t)$ and $R_f(M,n,q,t)$, which may imply better bounds via Theorem 2.1.

In the next two sections we apply these two approaches and obtain some bounds.

3. Bounds via analytical expressions of distance distributions

3.1. Preliminaries

Manev [18] obtained several different systems all equivalent to the systems from Theorem 1.3. These variants can facilitate faster computations or provide more convenient expressions. We will work the following set of systems (Theorem 7 in [18]).

Theorem 3.1 ([18]). *Let C be an $OA(M,n,q,t)$. All distance distributions from the sets $W(C) = P(C) \cup R(C)$ satisfy the system*

$$q^n \sum_{i=0}^{n} \binom{i-s}{m} w_i = M \sum_{i=0}^{n} \binom{n}{i} \binom{i-s}{m} (q-1)^i,\ m = 0,1,\ldots,t, \tag{5}$$

where $s \in \{0,\ldots,n-t\}$ is fixed.

Suitable choices of s for the system (5) allow good expression for important entries of the distance distributions. Using the system (5) for $s = n-t$ and multiplying both sides by the $(t+1) \times (t+1)$ nonsingular matrix with (i,j)-th entry $(-1)^{i+j}\binom{i}{j}$, $i,j \in \{0,1,\ldots,t\}$, we obtain the system

$$Bw^T = b := (b_0, b_1, \ldots, b_{t+1})^T. \tag{6}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 December 2021 doi:10.20944/preprints202112.0293.v1

Is was shown in [3] that the entries of the matrix B and the vector b can be explicitly computed as follows [2].

Theorem 3.2. a) *For $s = n - t$, the following equalities hold*

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

where $m \in \{0,1,\ldots,t\}$, $l \in \{0,1,\ldots,n\}$.

b) *For given $OA(M,n,q,t)$ and $s = n - t$, the following equalities hold*

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

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

$$b_0 = \lambda\binom{n}{t}, \quad b_1 = -\lambda\binom{n}{t-1}(n-t-q+1).$$

We will show below that combinations of these facts and expressions give general upper bounds for the quantities $MaxMD(M,n,q,t)$ and $CR(M,n,q,t)$.

In the end of this subsection we give a result which was used but not mentioned in [2].

Theorem 3.3. *Let M, n, q, and t be feasible parameters for orthogonal arrays in H_q^n and $f(z)$ be a real polynomial of degree at most t such that $f(z) \geq 0$ for every $z \in \{0,1,\ldots,n\}$. Then the elements of any distance distribution $w = [w_0, w_1, \ldots, w_n]$ with respect to a point $x \in H_q^n$ of any $OA(M,n,q,t)$ satisfy*

$$w_i \leq \left\lfloor \frac{f_0 M}{f(i)} \right\rfloor,$$

where

$$f_0 = \frac{1}{q^n}\sum_{j=0}^{n}\binom{n}{i}(q-1)^i f(i)$$

is the zeroth coefficient in the Krawtchouk expansion of $f(t)$.

Proof. Let $f(z) = f_0 + \sum_{j=0}^{t} f_j K_k^{n,q}(z)$ be the Krawtchouk expansion of $f(z)$. It is well known (and straightforward from (1)) that

$$\sum_{j=0}^{n} w_j f(j) = f_0 M.$$

Since all terms in the left hand side are nonnegative, we obtain the required inequality. □

The restrictions from the inequalities of Theorem 3.3 can be used for reducing the computational effort in the initial finding of the set $W_f(M,n,q,t)$. This becomes important for large parameters.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 December 2021 doi:10.20944/preprints202112.0293.v1

3.2. Upper bounds for the covering radius via distance distributions

The results, described in this subsection are now new, but reformulated from [3], where the authors apply Theorem 2.1 for obtaining upper bounds on the covering radius of OAs.

It is easy to see that the system (6) has a unique solution whose first $n-t$ coordinates are zeros, namely

$$r = [\underbrace{0,\ldots,0}_{n-t}, b_0, b_1, \ldots, b_{t+1}] \in R_f(M,n,q,t).$$

In particular, the exact values of b_0 and b_1 allow one to derive the upper bound

$$CR(M,n,q,t) \leq n-t \tag{7}$$

and its strengthening

$$CR(M,n,q,t) \leq n-t-1, \tag{8}$$

provided $n-t > q-1$ is fulfilled [3, Theorems III.4, III.5]. In the next step, the investigation of the distance distributions of OAs of related parameters, gives the stronger bound (obtained in [3])

$$CR(M,n,q,t) \leq n-t-2 \tag{9}$$

which is valid if the inequality $n > 2(t+q-1)$ is fulfilled. Examples with equality in all bounds (7)-(9) were shown in [3].

3.3. Upper bounds for the minimum distance via distance distributions

Theorem 2.1 was applied in [5] for the case $(M,n,q,t) = (96,10,2,4)$, where the set $P_f(96,10,2,4)$ was consecutively reduced to contain three distance distributions, all beginning with 1 followed by two zeros, meaning that $MinMD(96,10,2,4) = MaxMD(96,10,2,4) = 3$. In other words, every $OA(96,10,2,4)$ must have minimum distance of 3. However, this gives a contradiction to the Hamming bound and therefore proves that there exist no $OA(96,10,2,4)$.

The bound

$$MaxMD(M,n,q,t) \leq n-t+1$$

is well known (see, for example, [17]) and is attained by the maximum distance separable (MDS) codes. More precisely, the OAs of index $\lambda = 1$ are exactly the MDS codes (see Theorems 4.20 and 4.21 in [14]). Our first result in this section (Theorem 3.4 below) shows that our technique provides this classical bound.

The most convenient choice of s in Theorem 3.1 is again $s = n-t$, giving the system (6) again. In this case, we are interested in solutions of (6) which begin by 1 followed by several zeros.

Theorem 3.4. *Let C be an $OA(M,n,q,t)$ of index $\lambda > 1$ and minimum distance $d(C)$. Then*

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

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

$$p(x) = [\underbrace{1,0,\ldots,0}_{n-t}, p_{n-t}, \ldots, p_n],\ x \in C,$$

has $p_{n-t} \neq 0$. In fact, in this case the system (6) has a unique solution of this type and it is given by

$$p(x) = [\underbrace{1,0,\ldots,0}_{n-t}, b_0 - b_{0,0}, b_1 - b_{1,0}, \ldots, b_{t+1} - b_{t+1,0}].$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 December 2021 doi:10.20944/preprints202112.0293.v1

It follows from the expressions in Theorem 3.2 that

$$b_0 - b_{0,0} = \lambda\binom{n}{t} - \binom{n}{t} = \binom{n}{t}(\lambda - 1) > 0$$

whenever $\lambda > 1$. □

Remark 3.5. *In our interpretation, Theorem 3.4 shows that the condition $\lambda = 1$ is necessary and sufficient for $d(C) = n - t + 1$, and otherwise one has $d(C) \leq n - t$.*

Corollary 3.6. *For M, n, q, and t being feasible parameters for orthogonal arrays in H_q^n of index $\lambda > 1$, we have*

$$MaxMD(M, n, q, t) \leq n - t.$$

Similarly, to the covering radius situation, the investigation of the unique solution from the proof of Theorem 3.4 allows obtaining better bounds.

Theorem 3.7. *Let C be an $OA(M, n, q, t)$ of index $\lambda > 1$ and minimum distance $d(C)$. If $n - t > \frac{\lambda(q-1)}{\lambda-1}$, then $d(C) \leq n - t - 1$.*

Proof. Suppose that $d(C) = n - t$, i.e. the bound of Theorem 3.4 is achieved. Then the only solution of (6),

$$p(x) = (\underbrace{1, 0, \ldots, 0}_{n-t}, b_0 - b_{0,0}, b_1 - b_{1,0}, \ldots, b_{t+1} - b_{t+1,0}),$$

as discussed in the proof of Theorem 3.4, is the distance distribution of (every) internal point, where the minimum distance $n - t$ is realized. Therefore the numbers $b_i - b_{i,0}$, $i = 0, \ldots, n$, are nonnegative integers. However, computing via Theorem 3.4 gives

$$\begin{aligned} b_1 - b_{1,0} &= -\lambda\binom{n}{t-1}(n - t - q + 1) - (t - n)\binom{n}{t-1} \\ &= -\binom{n}{t-1}\Big(\lambda(n - t - q + 1) - n + t\Big) < 0 \end{aligned}$$

since $n - t > \frac{\lambda(q-1)}{\lambda-1}$. This contradiction shows that $d(C) = n - t$ is impossible, i.e. we have $d(C) = n - t - 1$. □

Corollary 3.8. *For n, M, q, and t being feasible parameters for orthogonal arrays in H_q^n of index $\lambda > 1$, we have*

$$MaxMD(M, n, q, t) \leq n - t - 1.$$

provided $n - t > \frac{\lambda(q-1)}{\lambda-1}$.

4. Bounds from databases

In the last several years we have created large databases with distance distributions for many sets of parameters with $q = 2$ [25] and $q = 3$ [26]. The initial sets are computed by using systems like (5) (derived from the Delsarte's (1) from Theorem 1.3). Then reducing results from [4–6] and other were applied and the bounds for $MinD(M, n, q, t)$, $MaxD(M, n, q, t)$ and $CR(M, n, q, t)$ were extracted via Theorem 2.1. In many cases we are able to find exact values despite the possibility of existence of many nonisomorphic versions of OAs with the corresponding parameters. We will appreciate any cooperation in this project.

Extended tables with bounds will soon appear in [25] and [26] for $q = 2$ and $q = 3$ (at this point we do not plan to proceed with larger q). Here we present two tables as a

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 December 2021 doi:10.20944/preprints202112.0293.v1

small portion of our results with some comments. In Table 1 we show bounds for $q = 2$ and $t = 2$, and in Table 3 bounds for $q = 2$ and larger strengths are listed.

Table 1. Some bounds for $MinD(M,n,2,2)$, $MaxD(M,n,2,2)$ and $CR(M,n,2,2)$ for some small values of n and M.

Strength t	Cardinality M	Length n	Minimum distance bounds	Covering radius bounds
t	2^t	$t+1$	2	1
t	2^{t+1}	$t+2$	1-2	1
t	2^{t+2}	$t+3$	1-2	1
2	8	5	2	1
2	8	6	3	2
2	8	7	4	3*
2	12	8	3	3
2	12	9	4	4
2	12	10	5	4
2	12	11	6	5*
2	16	12	5-6	5
2	16	13	6	5
2	16	14	7	6
2	16	15	8	7*
2	20	15	6-7	6
2	20	16	7	7
2	20	17	8	7
2	20	18	9	8
2	20	19	10	9*

Table 2. Some bounds for $MinD(M,n,2,t)$, $MaxD(M,n,2,t)$ and $CR(M,n,2,t)$ for $3 \leq t \leq 5$ and some small values of n and M.

Strength t	Cardinality M	Length n	Minimum distance bounds	Covering radius bounds
3	64	10	1-3	3
3	64	11	1-4	3
3	64	12	1-4	4
3	64	13	1-5	4
3	64	14	1-6	5
3	64	19	3-8	7
3	64	20	3-9	7
4	64	8	2	1
4	128	10	1-3	2
4	128	11	2-3	2
4	128	12	3-4	3
4	128	13	4	3
4	128	14	5	4
4	128	15	6	5*
5	128	9	2	1*

Key to the tables.

$*$ – the exists an OA which attains the corresponding bound (this list is far from complete);

The single values in the column with bound for the minimum distance mean that the upper and lower bounds coincide, i.e. every OA with the corresponding M, n, q, and t has this minimum distance.

Author Contributions: Conceptualization, writing–original draft preparation, supervision, PB; investigation, SB, PB, and MS; software, SB and MS. All authors have read and agreed to the published version of the manuscript.

Funding: The research of SB was supported, in part, by Sofia University contract 80-10-64/22.03.2021 and its continuation. The research of PB was supported in part by Bulgarian NSF project KP-06-Russia/33-2020. The research of MS was supported, in part, by Bulgarian NSF contract KP-06-N32/2-2019.

Conflicts of Interest: The authors declare no conflict of interest.

Data Availability Statement: Data supporting the results reported in Section 4 can be found in references [25] and [26].

References

1. Boumova, S.; Boyvalenkov, P.; Stoyanova, M. Orthogonal arrays, their distance distributions, minimum distance, and covering radius. submitted.
2. Boumova, S.; Ramaj, T.; Stoyanova M. Computing distance distributions of ternary orthogonal arrays. *Compt. Rend. Acad. Bulg. Sci.* **2021**, 74, 177–189.
3. Boumova, S.; Ramaj, T.; Stoyanova, M. On covering radius of orthogonal arrays. Proc. 17th International Workshop on Algebraic and Combinatorial Coding Theory, Bulgaria, 11-17 October, 2020, IEEE Xplore.
4. Boyvalenkov, P.; Kulina, H. Investigation of binary orthogonal arrays via their distance distributions. *Problems of Information Transmission* **2013**, 49, 320–330.
5. Boyvalenkov, P.; Kulina, H.; Stoyanova, M.; Marinova, T. Nonexistence of binary orthogonal arrays via their distance distributions. *Problems of Information Transmission* **2015**, 51, 326–334.
6. Boyvalenkov, P.; Marinova, T.; Stoyanova, M. Nonexistence of a few binary orthogonal arrays. *Discrete Applied Mathematics* **2017**, 217, 144–150.
7. Carter, J.; Wegman, M. Universal classes of hash functions. *Journal of Computer and System Sciences* **1979**, 18, 143–154.
8. Dawson, E.; Mahmoodian, E. Orthogonal arrays and ordered threshold schemes. *Australasian Journal of Combinatorics* **1993**, 8, 27–44.
9. Delsarte, Ph. Four fundamental parameters of a code and their combinatorial significance. *Inform. Contr.*, 1973, 23, 407-438.
10. Delsarte, Ph. An algebraic approach to the association schemes of coding theory. Philips Research Reports Supplements, No. 10, 1973.
11. Delsarte, Ph.; Levenshtein, V.I. Association schemes and coding theory. IEEE Trans. Inform. Theory, 1998, 44, 2477-2504.
12. Fazekas, G.; Levenshtein, V.I. On upper bounds for code distance and covering radius of designs in polynomial metric spaces. *Journal of Combinatorial Theory*, Ser. A, 70, 267-288, 1995.
13. Gopalakrishnan, K.; Stinson, D. Applications of orthogonal arrays to computer science. Ramanujan Mathematical Society, Lecture Notes Series in Mathematics 7 (2008) 149-164.
14. Hedayat, A.; Sloane, N.J.A.; Stufken, J. *Orthogonal Arrays: Theory and Applications*. Springer-Verlag, New York, 1999.
15. Koukouvinos, C.; Lappas, B.; Simos, D.E. Encryption schemes using orthogonal arrays. *Journal of Discrete Mathematical Sciences and Cryptography* 12 (2009) 615-628.
16. Levenshtein, V.I. Universal bounds for codes and designs. Chapter 6 (499-648) in *Handbook of Coding Theory*, Eds. V.Pless and W.C.Huffman, Elsevier Science B.V., 1998.
17. MacWilliams, F.J., Sloane, N.J.A. *The Theory of Error-Correcting Codes*. North Holland, Amsterdam, 1977.
18. Manev, N.L. On the distance distributions of orthogonal arrays. *Problems of Information Transmission* 56, 2020,
19. Stinson, D. Combinatorial characterizations of authentication codes. *Designs, Codes and Cryptography* 2 (1992) 175-187 (extended version of [20]).
20. Stinson, D. Combinatorial characterizations of authentication codes. Advances in Cryptology – CRYPT0'91 (Proceedings), Lecture Notes in Computer Science, Edited by G. Coos and J. Hartmanis, vol. 576, 1992.
21. Stinson, D. Combinatorial techniques for universal hashing. *Journal of Computer and System Sciences* 48 (1994) 337-346.
22. Szegő, G. *Orthogonal Polynomials*. AMS Col. Publ., 23, Providence, RI, 1939.
23. Tietäväinen, A. An upper bound on the covering radius as a function of the dual distance. *IEEE Trans. Inform. Theory*, 36(6):1472–1474, Nov 1990.
24. Tietäväinen, A. Covering radius and dual distance. *Des. Codes Cryptogr.*, 1, 31-46, 1991.
25. https://store.fmi.uni-sofia.bg/fmi/algebra/stoyanova/BOALibrary/BOA.html
26. https://store.fmi.uni-sofia.bg/fmi/algebra/stoyanova/TOALibrary/TOA.html