New nonexistence results for binary orthogonal arrays

MAYA STOYANOVA

Faculty of Mathematics and Informatics,

Sofia University "St. Kliment Ohridski", Sofia, Bulgaria

Joint work with:

Peter Boyvalenkov (Inst. Math. Inform., BAS, Sofia, Bulgaria),

Tanya Marinova (FMI, Sofia University, Sofia, Bulgaria)

15^{th} **International Workshop on Algebraic and Combinatorial Coding Theory, ACCT - 15, June 18-24, 2016, Albena, Bulgaria**

Orthogonal arrays

- Let $H(n,2)$ be the binary Hamming space of dimension n with usual Hamming distance.

Definition

An orthogonal array (OA) of strength τ and index λ in $H(n,2)$ (or BOA), consists of the rows of an $M \times n$ matrix C with the property that every $M \times \tau$ submatrix of C contains all ordered τ-tuples of $H(\tau,2)$, each one exactly $\lambda = M/2^\tau$ times as rows.

- index: $\lambda = M/2^\tau$,
- dimension: n, cardinality: $|C| = M$, strength: τ.
- We denote: $C - (n, M, \tau)$ BOA.

Main problem

Problem

For fixed strength τ and dimension n find the minimal possible cardinality M such that an orthogonal array of parameters (n, M, τ) exists in $H(n, 2)$, i.e. find

$$B(n, \tau) = min\{M : \ a\ (n, M, \tau) \text{ orthogonal array exists}\}.$$

- Since $M = \lambda 2^{\tau}$, the problem finding a lower bound for $B(n, \tau)$ is equivalent to the following problem:

Problem

For fixed strength τ and dimension n find the minimal possible index λ such that a $(n, M = \lambda 2^{\tau}, \tau)$ orthogonal array exists in $H(n, 2)$, i.e. find

$$L(n, \tau) = \min\{\lambda : \ a\ (n, M = \lambda 2^{\tau}, \tau) \text{ orthogonal array exists}\}.$$

Main bounds for $L(n, \tau)$

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

Table: (Table 12.1) Minimum possible index λ of binary orthogonal array of length n, $7 \leq n \leq 13$, and strength τ, $4 \leq \tau \leq 10$ up to BKMS results (2015)

n / τ	4	5	6	7	8	9	10
7	$^{sz}4$	2	1	1			
8	4^c	$^{sz}4$	2	1	1		
9	6, 7, 8	4^c	4	2	1	1	
10	$^{bkms}7, 8$	6, 7, 8	8^{kh}	4	2	1	1
11	$^{bkms}7, 8$	$^{bkms}7, 8$	8^c	8^{kh}	4	2	1
12	8^{bkms}	$^{bkms}7, 8$	12-16	8^c	8^{kh}	4	2
13	8	8^{bkms}	16	12-16	16^{kh}	8^{kh}	4

Distance distributions of an orthogonal array (1)

- Let $C \subset H(n,2)$ be an (n,M,τ) BOA.
- The distance distribution of C with respect to $c \in H(n,2)$ is the $(n+1)$-tuple

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

  where $w_i(c) = |\{x \in C | d(x,c) = i\}|$, $i = 0, \ldots, n$.
- Every distance distribution of C satisfies the system

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

  where $b_k = \frac{1}{2^n} \sum_{d=0}^{n} \binom{n}{d} \left(1 - \frac{2d}{n}\right)^k$ and, in particular, $b_k = 0$ for k odd.
- The number b_k is in fact the first coefficient in the expansion of the polynomial t^k in terms of (binary) Krawtchouk polynomials.

Distance distributions of an orthogonal array (2)

- Let n, M and $\tau \leq n$ be fixed.
- $P(n, M, \tau)$ - the set of all possible distance distributions of a (n, M, τ) BOA with respect to internal point $c \in C$;
- $Q(n, M, \tau)$ - the set of all possible distance distributions of a (n, M, τ) BOA with respect to external point $c \notin C$;
- Denote also $W(n, M, \tau) = P(n, M, \tau) \cup Q(n, M, \tau)$.
- We propose an algorithm which works on the sets $P(n, M, \tau)$, $Q(n, M, \tau)$ and $W(n, M, \tau)$ utilizing connections between related BOAs. During the implementation of our algorithm these sets are reduced until possible. However, we prefer to keep the initial notation in order to avoid tedious notation.

Relations between distance distributions of (n, M, τ) BOA and its derived BOAs (1)

Theorem

If the distance distribution $W = (w_0, w_1, \ldots, w_n)$ belongs to the set $W(n, M, \tau)$, then the distance distribution $\overline{W} = (w_n, w_{n-1}, \ldots, w_0)$ also belongs to $W(n, M, \tau)$.

Corollary

The distance distribution $W \in W(n, M, \tau)$ is ruled out if $\overline{W} \notin W(n, M, \tau)$.

- We proceed with analyzing relations between the BOA C and BOAs C' of parameters $(n-1, M, \tau)$ which are obtained from C by deletion of one of its columns.

Relations between distance distributions of (n, M, τ) BOA and its derived BOAs (2)

- It is convenient to fix the removing of the first column of C.
- $W \in W(n, M, \tau)$ - the distance distribution of C with respect to $c = \mathbf{0} \in H(n, 2)$,
- $W' = (w'_0, w'_1, \ldots, w'_{n-1}) \in W(n-1, M, \tau)$ - the distance distribution of C' with respect to $c' = \mathbf{0} \in H(n-1, 2)$,
- For every $i \in \{0, 1, \ldots, n\}$ the matrix which consists of the rows of C of weight i is called i-block. It follows from the above notations that the cardinality of the i-block is w_i.
- Denote by x_i (y_i, respectively) the number of the ones (zeros, respectively) in the intersection of the first column of C and the rows of the i-block.

Relations between distance distributions of (n, M, τ) BOA and its derived BOAs (3)

Theorem

The numbers x_i and y_i, $i = 0, 1, \ldots, n$, satisfy the following system of linear equations

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

Remark

The above Theorem was firstly proved and used in 2013 by Boyvalenkov-Kulina for $W \in P(n, M, \tau)$.

Relations between distance distributions of (n, M, τ) BOA and its derived BOAs (4)

Corollary

The distance distribution $W \in W(n, M, \tau)$ is ruled out if no system (1) obtained when W' runs $W(n-1, M, \tau)$ has a solution.

- The above Corollary rules out some distance distributions W but it mainly serves to produce feasible pairs (W, W') which will be investigated further.
- Property of BOAs: if we take the rows of C with first coordinate 0 (1, respectively) and remove that first coordinate then we obtain a BOA C_0 (C_1, respectively) of parameters $(n-1, M/2, \tau-1)$. At this stage the BOAs C_0 and C_1 have the same sets of admissible distance distributions – all these which have passed the sieves of previous two Corollaries for the set $W(n-1, M/2, \tau-1)$.

Relations between distance distributions of (n, M, τ) BOA and its derived BOAs (5)

$$
\begin{array}{c|c}
 & W' = (w'_0, w'_1, \ldots, w'_{n-1}) \\
 & C' - (n-1, M, \tau) \\
\hline
\begin{array}{c} 0 \\ 0 \\ \vdots \\ 0 \end{array} & \begin{array}{c} Y = (y_0, y_1, \ldots, y_{n-1}) \\ C_0 - (n-1, M/2, \tau - 1) \end{array} \\
\hline
\begin{array}{c} 1 \\ 1 \\ \vdots \\ 1 \end{array} & \begin{array}{c} X = (x_1, x_2, \ldots, x_n) \\ C_1 - (n-1, M/2, \tau - 1) \end{array} \\
\hline
\multicolumn{2}{c}{W = (w_0, w_1, \ldots, w_n)} \\
\multicolumn{2}{c}{C - (n, M, \tau)}
\end{array}
\qquad
\begin{array}{c|c}
 & W' \\
 & C' - (n-1, M, \tau) \\
\hline
\begin{array}{c} 1 \\ 1 \\ \vdots \\ 1 \end{array} & \begin{array}{c} Y \\ C_0 - (n-1, M/2, \tau - 1) \end{array} \\
\hline
\begin{array}{c} 0 \\ 0 \\ \vdots \\ 0 \end{array} & \begin{array}{c} X \\ C_1 - (n-1, M/2, \tau - 1) \end{array} \\
\hline
\multicolumn{2}{c}{\widehat{W} = (\widehat{w_0}, \widehat{w_1}, \ldots, \widehat{w_n})} \\
\multicolumn{2}{c}{C^{1,0} - (n, M, \tau)}
\end{array}
$$

Figure 1.

Relations between distance distributions of (n, M, τ) BOA and its derived BOAs (5)

Theorem

The distance distribution of the $(n-1, M/2, \tau-1)$ BOA C_0 with respect to c' is $Y = (y_0, y_1, \ldots, y_{n-1})$, i.e. $Y \in W(n-1, M/2, \tau-1)$.

- More precisely, we have two possibilities:
  if $y_0 \geq 1$, then $c' \in C_0$ and therefore $Y \in P(n-1, M/2, \tau-1)$,
  if $y_0 = 0$, then $c' \notin C_0$ and therefore $Y \in Q(n-1, M/2, \tau-1)$.

Corollary

The pair (W, W') is ruled out if $Y \notin W(n-1, M/2, \tau-1)$ or if $\overline{Y} = (y_{n-1}, y_{n-2}, \ldots, y_0) \notin W(n-1, M/2, \tau-1)$.

Relations between distance distributions of (n, M, τ) BOA and its derived BOAs (6)

Theorem

The distance distribution of the $(n-1, M/2, \tau-1)$ BOA C_1 with respect to c' is $X = (x_1, x_2, \dots, x_n)$, i.e. $X \in W(n-1, M/2, \tau-1)$.

- Similarly to above, we have two possibilities:
  if $x_1 \geq 1$, then $c' \in C_1$ and therefore $X \in P(n-1, M/2, \tau-1)$,
  if $x_1 = 0$, then $c' \notin C_1$ and therefore $X \in Q(n-1, M/2, \tau-1)$.

Corollary

The pair (W, W') is ruled out if $X \notin W(n-1, M/2, \tau-1)$ or if $\overline{X} = (x_n, x_{n-1}, \dots, x_1) \notin W(n-1, M/2, \tau-1)$.

Relations between distance distributions of (n, M, τ) BOA and its derived BOAs (7)

We consider the effect of the permutation $(0 \to 1, 1 \to 0)$ in the first column of C. We obtain a BOA $C^{1,0}$ of parameters (n, M, τ) again.

Theorem

If the distance distribution of C with respect to $c = \mathbf{0} \in H(n,2)$ is $W = (w_0, w_1, \ldots, w_{n-1}, w_n) = (y_0, x_1 + y_1, \ldots, x_{n-1} + y_{n-1}, x_n)$, then the distance distribution of $C^{1,0}$ with respect to c is $\widehat{W} = (x_1, x_2 + y_0, \ldots, x_n + y_{n-2}, y_{n-1})$, i.e. $\widehat{W} \in W(n, M, \tau)$.

Corollary

a) The pair (W, W') is ruled out if $\widehat{W} \notin W(n, M, \tau)$ or if $\overline{\widehat{W}} \notin W(n, M, \tau)$.
b) The distance distribution W is ruled out if all possible pairs (W, W'), where $W' \in W(n-1, M, \tau)$, are ruled out.

Relations between distance distributions of (n, M, τ) BOA and its derived BOAs (8)

Otherwise, we proceed with the remaining pairs as follows. Let

$$(x_0^{(j)} = 0, x_1^{(j)}, \ldots, x_n^{(j)}; y_0^{(j)}, y_1^{(j)}, \ldots, y_{n-1}^{(j)}, y_n^{(j)} = 0), \quad j = 1, \ldots, s, \qquad (2)$$

are all solutions coming from system (1) when W' runs $W(n-1, M, \tau)$ which have passed the sieves of all previous Corollaries. We now free the cutting and thus consider all possible n cuts of columns of C. These cuts produce pairs (W, W') (where W is fixed) and corresponding solutions (2). Let the solutions (2) appear with multiplicities $k_1, k_2, \ldots, k_s$, respectively.

Relations between distance distributions of (n, M, τ) BOA and its derived BOAs (9)

Theorem

The nonnegative integers $k_1, k_2, \ldots, k_s$ satisfy the system

$$\left| \begin{array}{llcclcl} k_1 & +k_2 & + & \cdots & +k_s & = n \\ k_1 x_1^{(1)} & +k_2 x_1^{(2)} & + & \cdots & +k_s x_1^{(s)} & = w_1 \\ k_1 x_2^{(1)} & +k_2 x_2^{(2)} & + & \cdots & +k_s x_2^{(s)} & = 2w_2 \\ & & & \ddots & & \\ k_1 x_n^{(1)} & +k_2 x_n^{(2)} & + & \cdots & +k_s x_n^{(s)} & = nw_n \end{array} \right. . \qquad (3)$$

Relations between distance distributions of (n, M, τ) BOA and its derived BOAs (10)

Corollary

The distance distribution W is ruled out if the system (3) does not have solutions.

Corollary

Let $j \in \{1, 2, \ldots, s\}$ be such that all solutions of the system (3) have $k_j = 0$. Then the pair (W, W'), which corresponds to j, is ruled out.

Applications of the algorithm

- All BOAs (in fact, their current sets P, Q and W) of interest for the targeted BOA $C = (n, M, \tau)$ are collected in a table:

$$(\tau, M, \tau)\ (\tau+1, M, \tau)\ (\tau+2, M, \tau)\ \ldots\ C = (n, M, \tau).$$

$$(\tau-1, M/2, \tau-1)\ (\tau, M/2, \tau-1)\ (\tau+1, M/2, \tau-1)\ \ldots\ (n-1, M/2, \tau-1)$$

  and so on until it makes sense.
- We apply Corollaries 6, 9b) and 10 in every row separately from left to right to reduce the sets P, Q and W. Of course, this process is fueled with information from the columns (starting from the bottom end) according to Corollaries 7, 8, 9a) and 11. Every nonsymmetric distance distribution W which is ruled out, forces its mirror image $\overline{W}$ to be ruled out according to Corollary 4.
- The algorithm stops when no new rulings out are possible. An entry at the right end, showing that some of the sets P, Q and W is empty means nonexistence of the corresponding BOA. Otherwise, we collect the reduced sets for further analysis and classification results.

New nonexistence results

Theorem

There exist no binary orthogonal arrays of parameters $(9, 96, 4)$ *and* $(10, 192, 5)$.

Theorem

There exist no binary orthogonal arrays of parameters $(10, 112, 4)$, $(11, 112, 4)$, $(11, 224, 5)$ *and* $(12, 224, 5)$.

An updated version of the Table

Table: (Table 12.1) Minimum possible index λ of binary orthogonal array of length n, $7 \leq n \leq 13$, and strength τ, $4 \leq \tau \leq 10$ up to BMS results (2016)

n / τ	4	5	6	7	8	9	10
7	${}^{sz}4$	2	1	1			
8	4^{c}	${}^{sz}4$	2	1	1		
9	${}^{bms}7$-8	4^{c}	4	2	1	1	
10	8^{bms}	${}^{bms}7$-8	8^{kh}	4	2	1	1
11	8^{bms}	8^{bms}	8^{c}	8^{kh}	4	2	1
12	8^{bkms}	8^{bms}	12-16	8^{c}	8^{kh}	4	2
13	8	8^{bkms}	16	12-16	16^{kh}	8^{kh}	4

THANK YOU FOR YOUR ATTENTION !

The research of the first author was supported, in part, by a Bulgarian NSF contract I01/0003.
The research of the second and third authors was supported, in part, by the Science Foundation of Sofia University under contract 57/2016.