Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 18-24, 2016, Albena, Bulgaria *pp. 90–95*

New nonexistence results for binary orthogonal arrays [1]

Peter Boyvalenkov peter@math.bas.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
8 G.Bonchev Street, 1113, Sofia, and Faculty of Mathematics and Natural Sciences,
South-Western University, Blagoevgrad, BULGARIA.

Tanya Marinova tanya.marinova@fmi.uni-sofia.bg
Maya Stoyanova stoyanova@fmi.uni-sofia.bg
Faculty of Mathematics and Informatics, Sofia University,
5 James Bourchier Blvd., 1164 Sofia, BULGARIA

Abstract. We prove the nonexistence of binary orthogonal arrays of parameters (length, cardinality, strength) = $(9, 6.2^4, 4)$, $(10, 6.2^5, 5)$, $(10, 7.2^4, 4)$, $(11, 7.2^5, 5)$, $(11, 7.2^4, 4)$ and $(12, 7.2^5, 5)$, resolving the first cases where the existence was undecided so far.

1 Introduction

Let $H(n, 2)$ be the binary Hamming space of dimension n with Hamming distance. An orthogonal array (OA) of strength τ and index λ in $H(n, 2)$ (or binary orthogonal array, 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.

Let $C \subset H(n, 2)$ be an (n, M, τ) BOA. The distance distribution of C with respect to $c \in H(n, 2)$ if the $(n+1)$-tuple $w = w(c) = (w_0(c), w_1(c), \ldots, w_n(c))$, where $w_i(c) = |\{x \in C | d(x, c) = i\}|$, $i = 0, \ldots, n$. All feasible distance distributions of BOA of parameters (n, M, τ) can be computed effectively for relatively small n and τ as shown in [1]. Indeed, every distance distribution of C satisfies the system

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

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

[1]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.

in terms of (binary) Krawtchouk polynomials (see [3, 5, 6]).

Let n, M and $\tau \le n$ be fixed. We denote by $P(n, M, \tau)$ the set of all possible distance distributions of a (n, M, τ) BOA with respect to internal point c (in the beginning – all admissible solutions of the system (1) with $w_0(c) \ge 1$) and by $Q(n, M, \tau)$ the set of all possible distance distributions of a (n, M, τ) BOA with respect to external point (in the beginning – all admissible solutions of the system (1) with $w_0(c) = 0$). 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 changed (reduced) until possible.

In Section 2 we prove several assertions which connect the distance distributions of arrays under consideration and their relatives. This allows us to collect rules for removing distance distributions from the sets $P(n, M, \tau)$, $Q(n, M, \tau)$ and $W(n, M, \tau)$. The logic of our algorithm and the new nonexistence results are described in Section 3.

Algorithms for dealing with distance distributions were proposed earlier in [1] and [2] but in these papers the set $P(n, M, \tau)$ was only examined. Moreover, two seemingly crucial observations (Theorem 1 together with Corollary 2 and Theorem 11 together with Corollary 11) are new. Also, the complete versions (for the set $W(n, M, \tau)$) of the remaining assertions are new.

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

First we will prove the following statement.

Theorem 1. *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 $W(n, M, \tau)$.*

Proof. Let $C \subset H(n, 2)$ be a BOA of parameters (n, M, τ) and $\overline{C}$ is the array which is obtained from C by the permutation $(0 \to 1, 1 \to 0)$ in the whole C. Since the distances inside C are preserved by this transformation, $\overline{C}$ is again (n, M, τ) BOA. On the other hand, distance i from external for C point to a point of C correspond to distance $n - i$ to the transformed point of $\overline{C}$. This means that if $w = (w_0, w_1, \ldots, w_n)$ is the distance distribution of C with respect to some point $c \in H(n, 2)$ (internal or external for C), then the distance distribution of $\overline{C}$ with respect to the same point (which can become either internal or external for $\overline{C}$, depending on whether $w_n > 0$ or $w_n = 0$) is $\overline{w} = (w_n, w_{n-1}, \ldots, w_0)$. □

Corollary 2. *The distance distribution $w \in W(n, M, \tau)$ is ruled out if $\overline{w} \notin W(n, M, \tau)$.*

Corollary 2 is important in all stages of our algorithm since it requires the non-symmetric distance distributions to be paired off and infeasibility of one element of the pair immediately implies infeasibility for the other.

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. Of course, the set $W(n-1, M, \tau)$ of possible distance distributions of C' is sieved by Corollary 2 as well.

It is convenient to fix the removing of the first column of C. Let the distance distribution of C with respect to $c = \mathbf{0} \in H(n, 2)$ be $w \in W(n, M, \tau)$ and the distance distribution of C with respect to $c' = \mathbf{0} \in H(n-1, 2)$ be $w' = (w'_0, w'_1, \ldots, w'_{n-1}) \in W(n-1, M, \tau)$.

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. Next we 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.

Theorem 3. *The numbers x_i and y_i, $i = 0, 1, \ldots, n$, satisfy the following system of linear equations*

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

Remark 4. *Theorem 3 was firstly proved and used in 2013 by Boyvalenkov-Kulina [1] for $w \in P(n, M, \tau)$.*

Corollary 5. *The distance distribution $w \in W(n, M, \tau)$ is ruled out if no system (2) obtained when w' runs $W(n-1, M, \tau)$ has a solution.*

Corollary 5 rules out some distance distributions w but it mainly serves to produce feasible pairs (w, w') which will be investigated further.

Our next step is based on the following 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 Corollaries 2 and 5 for the set $W(n-1, M/2, \tau-1)$.

We continue with relations between the BOAs C, C', C_0 and C_1 using the numbers x_i and y_i, $i = 0, 1, \ldots, n$.

Theorem 6. *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 in Theorem 6 – if $y_0 \geq 1$, then $c' \in C_0$ and therefore $y \in P(n-1, M/2, \tau-1)$ (this is Theorem 1a) in [2]), or $y_0 = 0$ when $c' \notin C_0$ and therefore $y \in Q(n-1, M/2, \tau-1)$.

Corollary 7. *The pair (w, w') is ruled out if $y \notin W(n-1, M/2, \tau-1)$ or if $\overline{y} = (y_{n-1}, y_{n-2}, \dots, y_0) \notin W(n-1, M/2, \tau-1)$.*

Theorem 8. *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 in Theorem 8 – if $x_1 \geq 1$, then $c' \in C_1$ and therefore $x \in P(n-1, M/2, \tau-1)$ (this is Theorem 2a) in [2]), or $x_1 = 0$ when $c' \notin C_1$ and therefore $x \in Q(n-1, M/2, \tau-1)$.

Corollary 9. *The pair (w, w') is ruled out if $x \notin W(n-1, M/2, \tau-1)$ or if $\overline{x} = (x_n, x_{n-1}, \dots, x_1) \notin W(n-1, M/2, \tau-1)$.*

In our next step we consider the effect of the permutation $(0 \to 1, 1 \to 0)$ in the first column of C. This transformation does not change the distances from C and thus we obtain a BOA $C^{1,0}$ of parameters (n, M, τ) again.

Theorem 10. *If the distance distribution of C with respect to $c = \mathbf{0} \in H(n, 2)$ is $w = (w_0, w_1, \dots, w_{n-1}, w_n) = (y_0, x_1 + y_1, \dots, x_{n-1} + y_{n-1}, x_n)$, then the distance distribution of $C^{1,0}$ with respect to c is $\widehat{w} = (x_1, x_2 + y_0, \dots, x_n + y_{n-2}, y_{n-1})$, i.e. $\widehat{w} \in W(n, M, \tau)$.*

Proof. There are x_i points in $C^{1,0}$ (coming from C_1) at distance $i-1$ from c. Analogously, there are y_i points in $C^{1,0}$ (coming from C_0) at distance $i+1$ from c. This means that the number of the points of $C^{1,0}$ at distance 0 from c is x_1, the number of the points of $C^{1,0}$ at distance i, $1 \leq i \leq n-1$, from c is $y_{i-1} + x_{i+1}$, and, finally, the number of the points of $C^{1,0}$ at distance n from c is y_{n-1}. Therefore the distance distribution of $C^{1,0}$ with respect to c is $\widehat{w} = (x_1, x_2 + y_0, \dots, x_n + y_{n-2}, y_{n-1})$. □

Corollary 11. *The pair (w, w') is ruled out if $\widehat{w} \notin W(n, M, \tau)$ or if $\overline{\widehat{w}} \notin W(n, M, \tau)$.*

Corollary 12. *The distance distribution w is ruled out if all possible pairs (w, w'), where $w' \in W(n-1, M, \tau)$, are ruled out.*

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

$$(x_0^{(j)} = 0, x_1^{(j)}, \dots, x_n^{(j)}; y_0^{(j)}, y_1^{(j)}, \dots, y_{n-1}^{(j)}, y_n^{(j)} = 0), \quad j = 1, \dots, s, \tag{3}$$

are all solutions coming from Theorem 3 when w' runs $W(n-1, M, \tau)$ which have passed the sieves of Corollaries 7, 9 and 11. 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 (3). Let the solutions (3) appear with multiplicities $k_1, k_2, \dots, k_s$, respectively.

Theorem 13. *[1] The nonnegative integers $k_1, k_2, \ldots, k_s$ satisfy the system*

$$\left| \begin{array}{llllll} k_1 & +k_2 & + & \cdots & +k_s & = n \\ k_1 x_1^{(1)} & +k_2 x_1^{(2)} & + & \cdots & +k_s x_1^{(s)} & = w_1 \\ k_1 x_2^{(1)} & +k_2 x_2^{(2)} & + & \cdots & +k_s x_2^{(s)} & = 2w_2 \\ & & & \ddots & & \\ k_1 x_n^{(1)} & +k_2 x_n^{(2)} & + & \cdots & +k_s x_n^{(s)} & = nw_n \end{array} \right. . \tag{4}$$

Proof. This follows for counting in two ways the number of the ones in the i-block of C. For fixed $i \in \{1, 2, \ldots, n\}$, this number is obviously iw_i, and, on the other hand, it is equal to the sum $k_1 x_i^{(1)} + k_2 x_i^{(2)} + \cdots + k_s x_i^{(s)}$. □

Corollary 14. *The distance distribution w is ruled out if the system (4) does not have solutions.*

Corollary 15. *Let $j \in \{1, 2, \ldots, s\}$ be such that all solutions of the system (4) have $k_j = 0$. Then the pair (w, w'), which corresponds to j, is ruled out.*

3 Applications of the algorithm and new nonexistence results

We organize the results from the previous section to work together as follows.

All BOAs (in fact, their current sets of feasible distance distributions P, Q and W) of interest for the targeted BOA $C = (n, M, \tau)$ are collected in a table starting with first row

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

The next row consist of the derived BOAs

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

and so on until it makes sense. We apply Corollaries 5, 12 and 14 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, 9, 11 and 15. Every nonsymmetric distance distribution w which is ruled out, forces its mirror image $\overline{w}$ to be ruled out according to Corollary 2.

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 (in some cases, possibly, uniqueness).

For a putative $(9, 96, 4)$ BOA our algorithm ends with empty set $W(9, 96, 4)$. Moreover, since $(n, N, 2k)$ and $(n + 1, 2N, 2k + 1)$ BOAs coexist [7] (see also [4, Theorem 2.24]), we obtain the following nonexistence result.

Theorem 16. *There exist no binary orthogonal arrays of parameters* $(9, 96, 4)$ *and* $(10, 192, 5)$.

Next application ends with empty $W(10, 112, 4)$ and $W(11, 112, 4)$.

Theorem 17. *There exist no binary orthogonal arrays of parameters* $(10, 112, 4)$, $(11, 112, 4)$, $(11, 224, 5)$ *and* $(12, 224, 5)$.

The new nonexistence results give improvements in six entries of Table 12.1 from [4]. We have $7 \leq L(n, \tau) \leq 8$ instead of $6 \leq L(n, \tau) \leq 8$ for the pairs $(n, \tau) = (9, 4)$ and $(10, 5)$ and also have $L(n, \tau) = 8$ instead of $7 \leq L(n, \tau) \leq 8$ for the pairs $(n, \tau) = (10, 4)$, $(11, 4)$, $(11, 5)$ and $(12, 5)$.

All calculations in this paper were performed by programs in Maple. All results (in particular all possible distance distributions in the beginning) can be seen at [8]. All programs are available upon request.

References

[1] P. Boyvalenkov, H. Kulina, Investigation of binary orthogonal arrays via their distance distributions, *Problems of Information Transmission*, **49(4)**, 320-330 (2013).

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

[3] P. Delsarte, V. I. Levenshtein, Association schemes and coding theory, *IEEE Trans. Inform. Theory*, **44**, 2477-2504 (1998).

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

[5] V. I. Levenshtein, Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces, *IEEE Trans. Infor. Theory*, **41**, 1303-1321 (1995).

[6] V. I. Levenshtein, 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).

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

[8] https://drive.google.com/folderview?id=0B0r6JtxqB_RmLXRVQTBnM ldmcGM&usp=sharing