Seventh International Workshop on Optimal Codes and Related Topics
September 6-12, 2013, Albena, Bulgaria *pp. 65-70*

Nonexistence of certain binary orthogonal arrays

Peter Boyvalenkov peter@moi.math.bas.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
8 G.Bonchev str., 1113, Sofia, BULGARIA

Hristina Kulina kulina@pu.acad.bg
Faculty of Mathematics and Informatics, Plovdiv University,
236 Bulgaria Blvd., 4003 Plovdiv, BULGARIA

Maya Stoyanova stoyanova@fmi.uni-sofia.bg
Faculty of Mathematics and Informatics, Sofia University,
5 James Bourchier blvd, 1164 Sofia, BULGARIA

Dedicated to the memory of Professor Stefan Dodunekov

Abstract. We prove that binary orthogonal arrays of strength 8, length 12 and cardinality 1536 do not exist. This implies the nonexistence of arrays of parameters (strength,length,cardinality) = $(n, n+4, 6.2^n)$ for every integer $n \geq 8$.

1 Introduction

Let $H(n,2)$ be the binary Hamming space of dimension n. A binary orthogonal array (BOA), or equivalently, a τ-design C in $H(n,2)$, is an $M \times n$ matrix of a code C such that every $M \times \tau$ submatrix contains all ordered τ-tuples of $H(\tau,2)$, each one exactly $\frac{|C|}{2^\tau}$ times as rows.

In [1, 2] the first two authors proposed method of investigation of BOAs via calculation of all possible distance distributions and then exploiting some known connections between similar arrays.

In this note we describe our results on the investigation of BOAs of parameters (strength,length,cardinality)= $(n, n+4, 6.2^n)$. We prove that such BOAs do not exist for every $n \geq 8$.

Our approach follows the ideas from [2] with one new result which allows ut to rule out certain last remaining cases.

2 Overview of the method of investigation

We consider BOAs of parameters such that all feasible distance distributions can be effectively calculated and stored for further use. The possibility for such calculations was described firstly by Delsarte [3] (see also [4, 6]). In fact we solve certain Vandermonde-type systems of linear equations [1].

Let C be a $(\tau, n, |C| = M)$ BOA. Having all feasible distance distributions of C we apply several algorithms to investigate whether certain relation are satisfied [2]. In fact, two algorithms, A and B, were proposed in [2] to exploit the connections between the distance distributions of distinct points of C and its relatives.

Algorithm A investigates what happens with the distance distributions when we cut one column of the matrix of C deriving some BOA C' of parameters $(\tau, n-1, M)$. Distance distributions of C and C' are connected and all possible connections can be described. We apply this in the sequence τ-(τ, M), τ-$(\tau+1, M)$, ..., τ-$(n-1, M)$, τ-(n, M) to reduce the number of the feasible distance distributions of the last entry, say C again.

Algorithm B is applied for investigation of the relations between C and its relatives derived by simultaneous cut of several columns (defined by the support of some point). This is further combined with relations which are sometimes specific for the BOA under consideration.

Here we add one more argument which uses the information from Algorithm A and one further relation between C and its related BOAs of parameters $(\tau-1, n-1, M/2)$.

3 Connections between (τ, n, M) and $(\tau-1, n-1, M/2)$ BOAs

In algorithm A we define the i-block of C, $i \in \{0, 1, \dots, n\}$, as the set of all rows of weight i in the matrix of C. Then for fixed column we define the numbers x_i and y_i to be the number of 0's and 1's, respectively, in the intersection of that column and the i-blok. The calculation of the numbers x_i and y_i, $i = 0, 1, \dots, n$, is one of the results of Algorithm A.

It is well known (cf. [5]) that if we order the first column of C to begin with $M/2$ zeros and cut that column then both the upper and the lower half of the new matrix constitute BOAs of parameters $(\tau-1, n-1, M/2)$.

Theorem 1. *a) The vector $(y_0, y_1, \dots, y_{n-1})$ coincides with some distance distribution of a point in a BOA of parameters $(\tau-1, n-1, M/2)$.*

b) The vector $(x_1, x_2, \dots, x_n)$ represents some distance distribution of a point in a BOA of parameters $(\tau-1, n-1, M/2)$ where the entries are rearranged under certain rule. In particular, when C contains a row of weight one and the cut column corresponds to the support of that row, then $(x_1, x_2, \dots, x_n)$ coincides with some distance distribution of a point in a BOA of parameters

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

Proof. a) Denote by D the upper half after the cut. Then the zero vector belongs to D. Therefore its distance distribution, which is obviously some distance distribution of a point in D (a BOA of parameters $(\tau-1, n-1, M/2)$), is given by the weights in D. However, it is easy to see that the weight distribution of D is exactly $(y_0, y_1, \ldots, y_{n-1})$.

b) Denote by E the lower half after the cut. Let u be the first row of E. For every point $v \in E$ at distance j from u and of weight i (this weight corresponds to weight $i+1$ in C, i.e. to the $(i+1)$-block) we have $j = d(u,v) = wt(u) + wt(v) - 2wt(u*v)$, whence $j - i = wt(u) - 2wt(u*v)$. The last formula defines the rule for rearrangement of the distance distribution of a point in a BOA of parameters $(\tau-1, n-1, M/2)$ to give the distance distribution of u in E. In particular, if $wt(u) = 0$ (this can be always achieved when C possesses a point of weight 1) we have $j - i = 0$, i.e. $(x_1, x_2, \ldots, x_n)$ itself is a distance distribution of a point in a BOA of parameters $(\tau-1, n-1, M/2)$. □

We show below how a) can be used but b) is not used in this note. We only notice that b) can be very useful for small weights of u. For example, if $wt(u) = 1$ then we have $j - i = -1$ or 1, which means that $(x_1, x_2, \ldots, x_n)$ can be obtained from some distance distribution of a point in a BOA of parameters $(\tau-1, n-1, M/2)$ by moving its coordinates by one position.

Theorem 1 combined with the results from Algorithm A allows the following argument.

1. Calculate all possible distance distributions of the targeted BOA (τ, n, M). Apply Algorithm A to reduce them. Collect the information of Algorithm A for the remaining distance distributions.

2. Calculate all possible distance distributions of BOA of parameters $(\tau-1, n-1, M/2)$. Apply Algorithm A to reduce them.

3. Fix a distance distribution of the targeted BOA (τ, n, M) and consider all distance distributions of its derived $(\tau, n-1, M)$ BOA (by cut of a column). Rule out all distance distributions of the derived BOA whose vectors $(y_0, y_1, \ldots, y_{n-1})$ from the results of 1. do not appear as results of 2.

4. Rule out the considered distance distribution of the targeted BOA (τ, n, M) if the results of 3. contradict to the results of Algorithm A (for example, if Algorithm A states that some distance distributions of the $(\tau, n-1, M)$ BOA should appear but 3. rules out that distance distribution).

4 Application for $(8, 12, 1536)$ BOA and consequences

We describe how the above algorithm works in the case of BOA of parameters $(8, 12, 1536)$. The existence of such BOAs is mentioned as undecided in Table 12.3 from the book [5].

1. We calculate all feasible distance distributions of (8,12,1536) and apply Algorithm A. This results in 5 remaining distance distributions, namely

$$\begin{aligned}
W_1 &= (1, 0, 36, 80, 135, 432, 168, 432, 135, 80, 36, 0, 1),\\
W_2 &= (1, 0, 38, 63, 198, 300, 336, 306, 177, 92, 18, 7, 0),\\
W_3 &= (1, 0, 39, 54, 234, 216, 462, 180, 261, 56, 27, 6, 0),\\
W_4 &= (1, 1, 29, 99, 114, 426, 210, 390, 141, 101, 17, 7, 0),\\
W_5 &= (1, 1, 30, 90, 150, 342, 336, 264, 225, 65, 26, 6, 0),
\end{aligned}$$

For every W_i we know all possible distance distributions of BOA of parameters (8,11,1536) which can appear after cut of a column and, moreover, we know how many times appears each of them. Explicitly, we have again 5 possibilities:

$$\begin{aligned}
V_1 &= (1, 5, 59, 69, 354, 210, 462, 186, 141, 41, 7, 1),\\
V_2 &= (1, 6, 50, 105, 270, 336, 336, 270, 105, 50, 6, 1),\\
V_3 &= (1, 7, 41, 141, 186, 462, 210, 354, 69, 59, 5, 1),\\
V_4 &= (1, 8, 33, 168, 138, 504, 210, 312, 117, 32, 13, 0),\\
V_5 &= (2, 0, 60, 120, 180, 504, 168, 360, 90, 40, 12, 0),
\end{aligned}$$

2. We calculate all feasible distance distributions of (7,11,768) and apply Algorithm A. This results in 5 remaining distance distributions, namely

$$\begin{aligned}
U_1 &= (1, 0, 30, 60, 90, 252, 84, 180, 45, 20, 6, 0),\\
U_2 &= (1, 0, 31, 52, 118, 196, 154, 124, 73, 12, 7, 0),\\
U_3 &= (1, 0, 32, 45, 138, 168, 168, 138, 45, 32, 0, 1),\\
U_4 &= (1, 1, 25, 65, 110, 182, 182, 110, 65, 25, 1, 1),\\
U_5 &= (1, 2, 18, 85, 82, 196, 196, 82, 85, 18, 2, 1),
\end{aligned}$$

3.1. For W_1 Algorithm A gives V_1, V_2 and V_3 as possibilities but V_3 has vector $(y_0, y_1, \ldots, y_{11})$ which is not in the list $U_1, \ldots, U_5$. Now V_1 and V_2 correspond to a unique solution which shows that V_1 can not appear but V_2 appears after cut of every column of the targeted (8,12,1536). Thus W_1 remains for further consideration.

3.2. For W_2 Algorithm A gives V_1, V_2 and V_4 as possibilities but V_1 has vector $(y_0, y_1, \dots, y_{11})$ which is not in the list $U_1, \dots, U_5$. On the other hand, V_1, V_2 and V_4 correspond to a unique solution which shows that all of them must appear after cut of a column of the targeted (8,12,1536). Therefore W_2 is ruled out.

3.3. For W_3 Algorithm A gives V_1, V_2, V_3 and V_4 as possibilities. Now V_1 and V_2 have vectors $(y_0, y_1, \dots, y_{11})$ which are not in the list $U_1, \dots, U_5$. On the other hand, V_1, V_2, V_3 and V_4 correspond to a unique solution which shows that V_1 must appear after cut of 6 columns of the targeted (8,12,1536). Therefore W_3 is ruled out.

3.4. For W_4 Algorithm A gives V_1, V_2, V_4 and V_5 as possibilities. Now V_2, V_4 and V_5 have vectors $(y_0, y_1, \dots, y_{11})$ which are not in the list $U_1, \dots, U_5$. On the other hand, V_1, V_2, V_4 and V_5 correspond to a unique solution which shows that all of them must appear after cut of a column of the targeted (8,12,1536). Therefore W_5 is ruled out.

3.5. For W_5 Algorithm A gives V_1, V_2, V_3, V_4 and V_5 as possibilities but V_1, V_3 and V_4 have vectors $(y_0, y_1, \dots, y_{11})$ which are not in the list $U_1, \dots, U_5$. On the other hand, V_1, V_2, V_3, V_4 and V_5 correspond to a unique solution which shows that V_1 and V_4 must appear after cut of a column of the targeted (8,12,1536). Therefore W_5 is ruled our.

Finally, only W_1 remains as possible distance distribution in $(8, 12, 1536)$. However, Algorithm B (cf. [2]) with $\tau_0 = 3$ implies that the points of weight 3 in such a BOA must have distance distribution W_3, which was ruled out above.

Theorem 2. *There exist no binary orthogonal arrays of parameters* $(n, n+4, 6.2^n)$ *for every integer* $n \geq 8$.

Proof. The above application of the algorithm from section 3 implies the nonexistence of BOAs of parameters $(8, 12, 1536)$. Now it is enough to note that the existence of a BOA of parameters (τ, n, M) imply the existence of a BOA with parameters $(\tau - 1, n - 1, M/2)$ by the construction described in the beginning of Section 2. □

Acknowledgments. The first author is also with South-Western University (Faculty of Mathematics and Natural Sciences), Blagoevgrad, Bulgaria. His research was supported by the Bulgarian NSF under Contract I01/0003. The research of the second author was partially supported by the project NI13 FMI-002, NPD of Plovdiv University. The research of the third author was supported by the SF of Sofia University under Contract 101/2013.

References

[1] P. Boyvalenkov, H. Kulina, Computing distance distributions of orthogonal arrays, Proc. 12th Intern. Workshop on algebraic and combinatorial coding theory, Novosibirsk, Russia, Sep. 2010, 82-85.

[2] P. Boyvalenkov, H. Kulina, Investigation of binary orthogonal arrays via their distance distributions, to appear.

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

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

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

[6] V. I. Levenshtein, 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.