Discrete Applied Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Nonexistence of a few binary orthogonal arrays

Peter Boyvalenkov [a,b,*], Tanya Marinova [c], Maya Stoyanova [c]

[a] Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 8 G Bonchev Str., 1113 Sofia, Bulgaria
[b] Faculty of Mathematics and Natural Sciences, South-Western University, Blagoevgrad, Bulgaria
[c] Faculty of Mathematics and Informatics, Sofia University, 5 James Bourchier Blvd., 1164 Sofia, Bulgaria

ARTICLE INFO

Article history:
Received 21 April 2016
Received in revised form 20 July 2016
Accepted 29 July 2016
Available online xxxx

Keywords:
Binary Hamming space
Orthogonal arrays
Krawtchouk polynomials
Distance distributions
Nonexistence

ABSTRACT

We develop and apply combinatorial algorithms for investigation of the feasible distance distributions of binary orthogonal arrays with respect to a point of the ambient binary Hamming space utilizing constraints imposed from the relations between the distance distributions of connected arrays. This turns out to be strong enough and we prove the nonexistence of binary orthogonal arrays of parameters (length, cardinality, strength) $=$ $(9, 96, 4)$, $(10, 192, 5)$, $(10, 112, 4)$, $(11, 224, 5)$, $(11, 112, 4)$ and $(12, 224, 5)$, resolving the first cases where the existence was undecided so far. For the existing arrays our approach allows substantial reduction of the number of feasible distance distributions which could be helpful for classification results (uniqueness, for example).

1. Introduction

Orthogonal arrays have many connections to other combinatorial designs and have applications in coding theory, the statistical design of experiments, cryptography, various types of software testing and quality control. We refer to the book [6] as excellent exposition of the theory and practice of orthogonal arrays. In fact, there are enormous material about orthogonal arrays in internet.

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 [2]. 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.

* Corresponding author at: Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 8 G Bonchev Str., 1113 Sofia, Bulgaria.
E-mail addresses: peter@math.bas.bg (P. Boyvalenkov), tanya.marinova@fmi.uni-sofia.bg (T. Marinova), stoyanova@fmi.uni-sofia.bg (M. Stoyanova).

http://dx.doi.org/10.1016/j.dam.2016.07.023
0166-218X/

The number b_k is in fact the first coefficient in the expansion of the polynomial t^k in terms of (binary) Krawtchouk polynomials. The Krawtchouk polynomials are zonal spherical functions for $H(n, 2)$ (see [5,8,9]) and can be the defined by the three-term recurrence relation

$$(n-k)Q_{k+1}^{(n)}(t) = ntQ_k^{(n)}(t) - kQ_{k-1}^{(n)}(t) \quad \text{for } 1 \le k \le n-1,$$

with initial conditions $Q_0^{(n)}(t) = 1$ and $Q_1^{(n)}(t) = t$.

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 $W(n, M, \tau) = P(n, M, \tau) \cup Q(n, M, \tau)$.

In this paper we describe 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[1] by ruling out some distance distributions.

In Section 2 we prove several assertions which connect the distance distributions of arrays under consideration and their relatives. This imposes significant constraints on the targeted BOAs and therefore 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 is described in Section 3. The new nonexistence results are described in Section 4.

Algorithms for dealing with distance distributions were proposed earlier in [2,3] 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 12 together with Corollary 13) are new. Also, all complete versions (for the set $W(n, M, \tau)$) of the remaining assertions from the next section are new.

After the book [6], the enumeration and existence/nonexistence of BOAs was also addressed in [1,4,7,10,12] by different methods and on different targets. Our results confirm the nonexistence claims from [4] for small lengths and from [7] for large lengths. It would be interesting if the remaining distance distributions can be compared.

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

We start with a simple observation.

Theorem 1. *If the distance distribution $w = (w_0, w_1, \dots, w_n)$ belongs to the set $W(n, M, \tau)$, then the distance distribution $\overline{w} = (w_n, w_{n-1}, \dots, w_0)$ 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 corresponds to distance $n - i$ to the transformed point of $\overline{C}$. This means that if $w = (w_0, w_1, \dots, w_n)$ 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 $\overline{w} = (w_n, w_{n-1}, \dots, w_0)$. □

Corollary 2. *The distance distribution $w = (w_0, w_1, \dots, w_n) \in W(n, M, \tau)$ is ruled out if $\overline{w} = (w_n, w_{n-1}, \dots, w_0) \notin W(n, M, \tau)$.*

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 the 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 $c = \mathbf{0} = (0, 0, \dots, 0) \in H(n, 2)$ be $w = (w_0, w_1, \dots, w_n) \in W(n, M, \tau)$ and the distance distribution of C with respect to $c' = (0, 0, \dots, 0) \in H(n - 1, 2)$ be $w' = (w'_0, w'_1, \dots, w'_{n-1}) \in W(n - 1, M, \tau)$.

For every $i \in \{0, 1, \dots, n\}$ 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, $i = 0, 1, \dots, n$, satisfy the following system of linear equations*

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

[1] However, we prefer to keep the initial notation in order to avoid tedious notation.

Please cite this article in press as: P. Boyvalenkov, et al., Nonexistence of a few binary orthogonal arrays, Discrete Applied Mathematics (2016), http://dx.doi.org/10.1016/j.dam.2016.07.023