Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 117–120*

Moments of 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@uni-plovdiv.bg
Faculty of Mathematics and Informatics, Plovdiv University,
236 Bulgaria Blvd., 4003 Plovdiv, BULGARIA

Abstract. We consider connections between the distance distributions and the moments of orthogonal arrays. We combine information which can be derived by polynomial techniques to obtain some characterization results.

1 Introduction

Let $H(n,2)$ be the binary Hamming space of dimension n. A binary orthogonal array (OA), or equivalently, a τ-design $C \in H(n,2)$, consists of the rows of an $M \times n$ matrix, $M = |C|$, such that every $M \times \tau$ submatrix contains all ordered τ-tuples of $H(\tau,2)$, each one exactly $\frac{M}{2^\tau}$ times as rows (in particular, M is divisible to 2^τ). The maximal τ with this property is called strength of the array. OA's are important in the statistics, experimental mathematics, etc. (see [4, 6]).

We consider $H(n,2)$ with the inner product $\langle x,y\rangle = 1 - \frac{2d(x,y)}{n}$, where $d(x,y)$ is the Hamming distance between x and y. Then an equivalent definition of OA (cf. [3, 6]) is convenient for the so called polynomial techniques.

Definition 1. *A code $C \subset H(n,2)$ is an OA of strength τ if and only if for every real polynomial $f(t)$ of degree at most τ and every point $x \in H(n,2)$ the equality*

$$\sum_{y\in C} f(\langle x,y\rangle) = f_0|C| \qquad (1)$$

holds, where f_0 is the first coefficient in the expansion $f(t) = \sum_{i=1}^{n} f_i Q_i^{(n)}(t)$, $Q_i^{(n)}(t)$ are the normalized Krawtchouk polynomials, i.e. $Q_i^{(n)}(1) = 1$ and explicitly

$$Q_i^{(n)}(t) = \frac{1}{\binom{n}{i}} \sum_{j=0}^{i} (-1)^j \binom{d}{j}\binom{n-d}{i-j},\ i = 0,1,\dots,n,$$

where $d = \frac{n(1-t)}{2}$ *[1, 3, 6].*

The Krawtchouk polynomials are the so-called zonal spherical functions for $H(n,s)$ and play very important role in obtaining characterizations of codes and designs in $H(n,2)$. This can be justified, for example, by the identity

$$|C|f(1) + \sum_{x,y \in C, x \neq y} f(\langle x,y \rangle) = |C|^2 f_0 + \sum_{i=1}^{n} \frac{f_i}{r_i} \sum_{j=1}^{r_i} \left(\sum_{x \in C} v_{ij}(x) \right)^2, \qquad (2)$$

which holds for every real polynomial $f(t) = \sum_{i=1}^{n} f_i Q_i^{(n)}(t)$ of degree at most n. Here $r_i = \binom{n}{i}$, $v_{ij}(x)$ are certain Boolean functions (cf. [5,6]).

Definition 2. *The numbers* $M_i = \frac{1}{r_i} \sum_{j=1}^{r_i} \left(\sum_{x \in C} v_{i,j}(x) \right)^2$, $1 \leq i \leq n$, *are called moments of* C*.*

The moments and the strength are connected by the fact that C is OA of strength τ if and only if $M_i = 0$ for $i = 1, 2, \ldots, \tau$. Also, one has $M_i = 0$ for every odd i if and only if C is antipodal (i.e. $x \in C$ implies $-x \in C$).

2 Basic properties of the moments

We describe some properties of the moments which follow from Definition 2 and the identity (2). Assume that $C \subset H(n,2)$ is a τ-design.

Theorem 1. *We have* $M_i = |C| + \sum_{x,y \in C, x \neq y} Q_i(\langle x,y \rangle)$ *for every* $i = 1, 2, \ldots, n$.

Proof. We set $f(t) = Q_i(t)$ in (2). Since $f_i = 1$ and $f_j = 0$ for $j \neq i$ and $Q_i(1) = 1$ from the normalization, the assertion follows. □

In particular, every moment M_i is a rational number whose denominator is a divisor of the LCM of all denominators of the coefficients of $Q_i(t)$.

Denote $t_j = -1 + \frac{2j}{n}$ and $k_j = |\{(x,y) : \langle x,y \rangle = t_j\}|$, $j = 0, 1, \ldots, n$. Since all possible inner products are finitely many, we can easily obtain further identities and bounds for the moments using in (2) polynomials with zeros in many t_j's.

Theorem 2. *Let* $f(t) = \prod_{j=0}^{n-1} (t - t_j) = \sum_{i=0}^{n} f_i Q_i^{(n)}(t)$*. Then*

$$\sum_{i=\tau+1}^{n} f_i M_i = |C|(f(1) - f_0|C|).$$

Proof. We set $f(t)$ in (2) and use that $f(t_j) = 0$ for $j = 0, 1, 2, \dots, n-1$, and $M_i = 0$ for $i = 1, 2, \dots, \tau$. □

The next assertion counts some impact of the structure of C relaxing the conditions on the polynomials used in (2).

Theorem 3. *Let the polynomial $f(t) = \sum_{i=0}^{k} f_i Q_i^{(n)}(t)$ of degree $k = n-1$ or n vanishes at all but one of the points $t_0, t_1, \dots, t_{n-1}$, say $f(t_j) \neq 0$. Then*

$$\sum_{i=\tau+1}^{k} f_i M_i = |C|(f(1) - f_0|C|) + k_j f(t_j).$$

Proof. We set $f(t)$ in (2) and use that $f(t_\ell) = 0$ for $\ell \neq j$, and $M_i = 0$ for $i = 1, 2, \dots, \tau$. □

Theorem 3 can be further generalized to include more k_j's. Similar assertions can be combined with information on the distance distribution of C. Indeed, Definition 1 allows calculation of all possible distance distributions of C (with respect to fixed point [2]) and, similarly, (2) can be used for obtaining all possible $(k_0, k_1, \dots, k_{n-1})$.

For example, if $n = 10$, $\tau = 5$ and $M = 192$ (the first open case for $\tau = 5$ in the table of the book [4]) we obtain $k_0 \in A = \{144, 146, \dots, 192\}$. Further, for every $k_0 \in A$, the even number k_9 satisfies $0 \leq k_9 \leq r$, where $r = k_0 - 144$. Similarly, all possible values of all other k_i's can be found.

3 Orthogonal arrays and spherical codes

There is standard transformation from the binary Hamming space $H(n, 2)$ to the Euclidean sphere $\mathbb{S}^{n-1}$ given by $1 \to 1/\sqrt{n}$ and $0 \to -1/\sqrt{n}$ in each coordinate. For given τ-design $C \subset H(n, 2)$ we denote by $\overline{C}$ its realization as spherical code under the above transformation.

For $\mathbb{S}^{n-1}$ viewed as polynomial metric space the Gegenbauer polynomials are the counterparts of the Krawtchouk polynomials in $H(n, 2)$. In particular, the counterpart of the identity (2) is valid.

Theorem 4. *If $\tau \geq 3$ then $\overline{C}$ is has at least strength 3 as a spherical design. Moreover, all moments M_i, $i = 4, 5, \dots, \tau$, of $\overline{C}$ as a spherical design can be calculated.*

Proof. The first assertion follows from the fact that the first four (up to degree 3) Gegenbauer and Krawtchouk polynomials coincide and Theorem 1 and its counterpart for $\mathbb{S}^{n-1}$ can be applied. For the second assertion, we set in (2) $f(t) = t^i$ for $i = 4, 5, \ldots, \tau$ and use the observation that the left hand sides of the obtained equalities coincide. Then we equate the right hand sides to calculate consecutively the moments M_4, M_5, etc. of $\overline{C}$. □

Consider again the case $n = 10$, $\tau = 5$ and $M = 192$ – it gives a spherical 3-design on $\mathbb{S}^9$ with moments $M_4 \approx 187,671$ and $M_5 = 0$. Further, for the smallest $k_0 = 144$ we have unique solution for all other k_i, $i = 1, \ldots, 9$ and this implies $M_6 \approx 389,366$, $M_7 \approx 55,4352$, $M_8 \approx 326,391$, etc, At the other end, for $k_0 = 192$, we obtain an antipodal spherical code with $M_i = 0$ for all odd i.

References

[1] M. Abramowitz, I. Stegun, *Handbook of Mathematical Functions*, Dover, New York, 1965.

[2] P. Boyvalenhkov, H. Kulina, Computing distance distributions of orthogonal arrays, Proc. 12th Intern. Workshop ACCT, Novosibirsk, Russia, 2010, 82-85.

[3] G. Fazekas, V. I. Levenshtein, On the upper bounds for code distance and covering radius of designs in polynomial metric spaces, *J. Comb. Theory A*, 70, 1995, 267-288.

[4] A. S. Hedayat, N. J. A. Sloane, J. Stufken, *Orthogonal Arrays: Theory and Applications*, Springer-Verlag, NY, 1999.

[5] V. I. Levenshtein, Bounds for packings in metric spaces and certain applications, *Probl. Kibern.* 40, 1983, 44-110 (in Russian).

[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.