

On the structure of binary orthogonal arrays with small covering radius

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

Abstract. We obtain restrictions on the structure of binary orthogonal arrays of strength 5 under the assumption that their covering radius is close to the Fazekas-Levenshtein bound. We obtain lower and upper bounds on the number of the points of the array which are closest to a point of realization of the covering radius.

1 Introduction

Let $H(n, 2)$ be the binary Hamming space of dimension n . An orthogonal array, 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. It is well known that the strength is equal to the dual distance of C minus one.

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 . An equivalent definition of a τ -designs (cf. [2, 3]) is convenient for the so called polynomial techniques.

Definition 1. A code $C \subset H(n, 2)$ is a τ -design in $H(n, 2)$ if and only if every real polynomial $f(t)$ of degree at most τ and every point $y \in H(n, 2)$ satisfy

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

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.

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

where $d = n(1 - t)/2$ [1, 2, 3].

Definition 2. The number $\rho(C) = \max_{y \in H(n,2)} \min_{x \in C} d(x, y)$ is called covering radius of C .

We work with the covering radius in terms of the inner products as $t_c = 1 - \frac{2\rho(C)}{n} = \min_{y \in H(n,2)} \max_{x \in C} \langle x, y \rangle$ which will be also called covering radius of C .

Fazekas-Levenshtein [2, Theorem 2] obtain the following lower bound on t_c (i.e. upper bound on $\rho(C)$): if C is a $(2k - \varepsilon)$ -design, then

$$t_c \geq t_{FL} = t_k^{0,1-\varepsilon}, \quad (2)$$

where $t_k^{0,1-\varepsilon}$ is the largest zero of certain polynomial.

Denote by $p_c(y)$ the number of the points $x \in C$ such that $t_c = \langle x, y \rangle = t_{|C|}(y)$. So y is a point in $H(n, 2)$ where the covering radius is attained – so called deep hole of C . In this note we consider designs with covering radius which is close to the bound t_{FL} and obtain bounds on $p_c(y)$ for every possible y .

2 Bounds on $p_c(y)$

For every real number a we denote by $[a]^{(n)}$ the minimum number $-1 + \frac{2\ell}{n}$, $\ell \in \mathbb{Z}$, which is greater than or equal to a and, similarly, by $[a]_{(n)}$ the maximum number $-1 + \frac{2\ell}{n}$, $\ell \in \mathbb{Z}$, which is less than or equal to a . Therefore the Fazekas-Levenshtein bound (2) states $t_c \geq [t_{FL}]^{(n)}$.

For $y \in H(n, 2)$ we define the (possibly) multiset

$$I(y) = \{\langle x, y \rangle : x \in C\} = \{t_1(y), t_2(y), \dots, t_{|C|}(y)\},$$

where $-1 \leq t_1(y) \leq t_2(y) \leq \dots \leq t_{|C|}(y) \leq 1$. It is clear that we can order the points of C to achieve the ordering of $I(y)$ as required. In what remains, the point y will be a point $y \in H(n, 2)$, where the covering radius is realized, i.e. $t_{|C|}(y) = t_c$.

The next theorem gives a lower bound on $p_c(y)$ for designs whose covering radius is as close as possible to t_{FL} .

Theorem 1. Let $C \subset H(n, 2)$ be a τ -design with covering radius $t_c = [t_{FL}]^{(n)}$. Let $f(t)$ be a real polynomial of degree at most τ such that $f(t) \leq 0$ for $t \in [-1, t_c - \frac{2}{n}]$ and $f(t)$ is increasing in $[t_c - \frac{2}{n}, t_c]$. Then

$$p_c(y) \geq \frac{f_0|C|}{f(t_c)}$$

for every admissible y .

Proof. It follows by (1) and the conditions of the theorem that

$$f_0|C| = \sum_{i=1}^{|C|} f(t_i(y)) \leq p_c(y)f(t_c).$$

Since $f(t_c) > 0$, it follows that $p_c(y) \geq \frac{f_0|C|}{f([t_{FL}]^{(n)})}$.

If we relax the condition on t_c , then we can obtain only upper bounds on $p_c(y)$.

Theorem 2. *Let $C \subset H(n, 2)$ be a τ -design with covering radius $t_c \geq [t_{FL}]^{(n)}$. Let $f(t)$ be a real polynomial of degree at most τ such that $f(t) \geq 0$ for $t \in [-1, 1]$ and $f(t)$ is increasing in $[t_{FL}]^{(n)}, 1]$. Then*

$$p_c(y) \leq \frac{f_0|C|}{f(t_c)}$$

for every admissible y .

Proof. Similar to Theorem 1.

As usually in the polynomial techniques, the polynomials in Theorems 1 and 2 have some free parameters which must be optimized. For small degrees (strengths) this is a routine calculation which can be performed by Maple or Mathematica.

3 Some applications

To avoid trivial case we give examples with $\tau = 5$ (where trivial cases also occur, indeed).

We apply Theorem 1 with polynomials $f(t) = (t - [t_{FL}]^{(n)} + \frac{2}{n})(t^2 + at + b)^2$, where a and b will be determined in a way to satisfy the conditions for $f(t)$ and to maximize the function $F(a, b) = \frac{f_0|C|}{f(t_c)}$, $t_c = [t_{FL}]^{(n)}$. The maximum is obtained for

$$a_1 = \frac{4(n-1)(n-2k-2)(n-2k-1)(n-2k)}{A},$$

$$b_1 = -\frac{(6+8k+4k^2-7n-4kn+n^2)(2+4k^2-3n-4kn+n^2)}{A},$$

where $A = n(n^4 - 4n^3(2k+1) + n^2(24k^2 + 24k + 5) - 2n(16k^3 + 24k^2 + 4k + 1) + 8k(2k^3 + 4k^2 + k - 1))$. The explicit form of $F(a_1, b_1)$ is too long to be stated here.

We consider Theorem 2 for polynomials $f(t) = (t+1)(t^2 + at + b)^2$, where a and b will be determined in a way to satisfy the conditions for $f(t)$ and to

minimize the function $G(a, b) = \frac{f_0|C|}{f(t_c)}$, $t_c = 1 - \frac{2k}{n}$. Our calculations show that the minimum is obtained for

$$a_2 = \frac{4k(n-2k)}{n(2+4k+4k^2-3n-4kn+n^2)},$$

$$b_2 = -\frac{(n-2)(2+4k^2-3n-4kn+n^2)}{n^2(2+4k+4k^2-3n-4kn+n^2)}$$

and is equal to

$$G(a_2, b_2) = \frac{n(n-1)(n-2)|C|}{(n-k)B},$$

where $B = n^4 - 4n^3(2k+1) + n^2(24k^2+24k+7) - 8n(4k^3+6k^2+2k+1) + 4(4k^4+8k^3+4k^2+1)$.

It is worth to note that for length $n = 9$, there is a coincidence $t_c = [t_{FL}]^{(n)}$. The upper and lower bounds by Theorems 1 and 2 also coincide and, moreover, give non-integral values. Therefore the bound $[t_{FL}]^{(n)}$ can not be attained. One possible value for t_c remains and this gives the exact value of the covering radius $\rho(C) = 1$.

In other cases, we obtain lower and upper bounds for p_c . Such bounds can be used for reducing the number of different cases in the following approach. We set $f(t) = 1, t, \dots, t^5$ in (1) and obtain a system of linear equations with unknowns – the numbers of the distance distribution of C with respect to y . There are finitely many candidates for solutions of this system and their number is substantially reduced by using the restrictions on p_c . One preliminary step reduces the possible values of $p_{t_c-2/n}(y) = |\{x \in C : \langle x, y \rangle = t_c - \frac{2}{n}\}|$ by using the inequality

$$f_0|C| = \sum_{i=0}^{|C|} f(t_i(y)) \geq p_{t_c-2/n}(y)f(t_c - \frac{2}{n}) + p_c(y)f(t_c),$$

where $f(t) = (t+1)(t^2+at+b)^2$ is as in Theorem 2. This implies

$$p_{t_c-2/n}(y) \leq \frac{f_0|C| - p_c(y)f(t_c)}{f(t_c - 2/n)}.$$

For example, for $n = 10$ and $|C| = 192$, under the assumption $t_c = [t_{FL}]^{(n)} = \frac{3}{5}$, we obtain $16 \leq p_c \leq 21$ by the above calculations (applications of Theorems 1 and 2).

The corresponding systems for $p_c = 16, 17$ and 21 do not have integer solutions and we conclude that $18 \leq p_c \leq 20$. In these cases we obtain six

solutions in total. In particular, we obtain no solutions with inner product -1 , which means that $-y \notin C$ for any choice of y .

Acknowledgments. This research was partially supported by the Bulgarian NSF under Contract MM-1405/04.

References

- [1] M. Abramowitz, I. Stegun, *Handbook of Mathematical Functions*, Dover, New York, 1965.
- [2] 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.
- [3] 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.