Sixth International Workshop on
Optimal Codes and Related Topics

On the structure of binary orthogonal arrays with small covering radius

Peter Boyvalenkov, Hristina Kulina

Varna, BULGARIA, June 16-22, 2009

Orthogonal array

- $H(n, 2)$ - binary Hamming space of dimension n.

Orthogonal array

- $H(n,2)$ - 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.

Orthogonal array

- $H(n,2)$ - 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.
- $\tau = d^\perp(C) - 1$.

Orthogonal array

- $H(n,2)$ - 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.
- $\tau = d^{\perp}(C) - 1$.
- We consider $H(n,2)$ with the inner product

$$\langle x,y \rangle = 1 - \frac{2d(x,y)}{n}, \tag{1}$$

where $d(x,y)$ is the Hamming distance between x and y.

Orthogonal array

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

$$\sum_{x \in C} f(\langle x, y \rangle) = f_0 |C|, \tag{2}$$

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.

Covering radius

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.

Covering radius

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 $t_c = 1 - \frac{2\rho(C)}{n} = \min_{y \in H(n,2)} \max_{x \in C} \langle x, y \rangle$.

Covering radius

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 $t_c = 1 - \frac{2\rho(C)}{n} = \min_{y \in H(n,2)} \max_{x \in C} \langle x, y \rangle$.
- 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

$$t_c \geq t_{FL} = t_k^{0,1-\varepsilon}, \qquad (3)$$

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

Bounds on $p_c(y)$

- $p_c(y) = |\{x | x \in C : t_c = \langle x, y \rangle\}|$, where y is a point in $H(n, 2)$ where the covering radius is attained.

Bounds on $p_c(y)$

- $p_c(y) = |\{x|x \in C : t_c = \langle x, y\rangle\}|$, where y is a point in $H(n,2)$ where the covering radius is attained.
  For every real number a we denote:
- $[a]^{(n)} = min\{-1 + \frac{2\ell}{n}, \ell \in \{0,1,\ldots,n\}$, which is greater than or equal to $a\}$
- $[a]_{(n)} = max\{-1 + \frac{2\ell}{n}, \ell \in \{0,1,\ldots,n\}$, which is less than or equal to $a\}$.

Bounds on $p_c(y)$

- $p_c(y) = |\{x|x \in C : t_c = \langle x, y\rangle\}|$, where y is a point in $H(n,2)$ where the covering radius is attained.
  For every real number a we denote:
- $[a]^{(n)} = min\{-1 + \frac{2\ell}{n}, \ell \in \{0,1,\dots,n\}$, which is greater than or equal to $a\}$
- $[a]_{(n)} = max\{-1 + \frac{2\ell}{n}, \ell \in \{0,1,\dots,n\}$, which is less than or equal to $a\}$.
- Therefore the Fazekas-Levenshtein bound (3) states $t_c \geq [t_{FL}]^{(n)}$.

Bounds on $p_c(y)$

- $p_c(y) = |\{x | x \in C : t_c = \langle x, y \rangle\}|$, where y is a point in $H(n,2)$ where the covering radius is attained.
  For every real number a we denote:
- $[a]^{(n)} = min\{-1 + \frac{2\ell}{n}, \ell \in \{0, 1, \dots, n\}$, which is greater than or equal to $a\}$
- $[a]_{(n)} = max\{-1 + \frac{2\ell}{n}, \ell \in \{0, 1, \dots, n\}$, which is less than or equal to $a\}$.
- Therefore the Fazekas-Levenshtein bound (3) states $t_c \geq [t_{FL}]^{(n)}$.
- For example if $\tau = 5$, $t_{FL} = \frac{\sqrt{3n-2}}{n}$.
- $n = 7, t_{FL} = \frac{\sqrt{19}}{7} \approx 0.6227, [t_{FL}]^{(n)} = \frac{5}{7} \approx 0.714286;$
- $n = 8, t_{FL} = \frac{\sqrt{11}}{4\sqrt{2}} \approx 0.586302, [t_{FL}]^{(n)} = \frac{3}{4} = 0.75;$
- $n = 10, t_{FL} = \frac{\sqrt{7}}{5} \approx 0.52915, [t_{FL}]^{(n)} = \frac{3}{5} = 0.6.$

Bounds on $p_c(y)$

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

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

where $-1 \le t_1(y) \le t_2(y) \le \cdots \le t_{|C|}(y) \le 1$. With y as above, we have $t_{|C|}(y) = t_c < 1$.

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 $f(t) \le 0$ for $t \in [-1, t_c - \frac{2}{n}]$ and $f(t)$ is increasing in $[t_c - \frac{2}{n}, t_c]$. Then

$$p_c(y) \ge \frac{f_0|C|}{f(t_c)} \tag{4}$$

for every admissible y.

Bounds on $p_c(y)$

Proof Theorem 1.

It follows by (2) 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 $p_c(y) \geq \frac{f_0|C|}{f([t_{FL}]^{(n)})}$. $\square$

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

$$p_c(y) \leq \frac{f_0|C|}{f(t_c)} \tag{5}$$

for every admissible y.

Bounds on $p_c(y)$

Proof Theorem 2.

It follows by (2) and the conditions of the theorem that

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

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

Some applications

Let $\tau = 5$.

- We apply Theorem 1 with polynomials $f(t) = (t - [t_{FL}]^{(n)} + \frac{2}{n})(t^2 + at + b)^2$ and maximize the function $F(a,b) = \frac{f_0|C|}{f(t_c)} = 1 - \frac{2k}{n}$, $t_c = [t_{FL}]^{(n)}$. 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 $A = n(n^4 - 4n^3(2k+1) + n^2(24k^2+24k+5) - 2n(16k^3+24k^2+4k+1) + 8k(2k^3+4k^2+k-1)$.

Some applications

- We consider Theorem 2 for polynomials $f(t) = (t+1)(t^2 + at + b)^2$ and minimize the function $G(a, b) = \frac{f_0|C|}{f(t_c)}$, $t_c = 1 - \frac{2k}{n}$.

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

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

and is equal to

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

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

Some applications

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 (2) 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.

Some applications

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 $|C| = 192$ (this is open case), 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).

Some applications

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.

Some applications

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.

- One solution is:
  $p_c = p_{\frac{3}{5}} = 18$; $p_{\frac{2}{5}} = 13$;
  $p_{\frac{1}{5}} = 24$; $p_0 = 87$;
  $p_{-\frac{1}{5}} = 10$; $p_{-\frac{2}{5}} = 27$;
  $p_{-\frac{3}{5}} = 12$; $p_{-\frac{4}{5}} = 1$; $p_{-1} = 0$.

Some applications

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.

- One solution is:
  $p_c = p_{\frac{3}{5}} = 18;\ p_{\frac{2}{5}} = 13;$
  $p_{\frac{1}{5}} = 24;\ p_0 = 87;$
  $p_{-\frac{1}{5}} = 10;\ p_{-\frac{2}{5}} = 27;$
  $p_{-\frac{3}{5}} = 12;\ p_{-\frac{4}{5}} = 1;\ p_{-1} = 0.$
- In particular, we obtain no solutions with inner product -1, which means that $-y \notin C$ for any choice of y.

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.

Thank you for your attention!