Computing distance distribution of orthogonal arrays

Peter Boyvalenkov, Hristina Kulina

ACCT, Novosibirsk, September 05 - 11, 2010

Introduction

- **Definition 1.** Orthogonal array (equivalently, a τ-design) – an $M \times n$ matrix C in $H(n,2)$ such that every $M \times \tau$ submatrix of C contains all ordered τ-tuples, each one exactly $\frac{|C|}{2^\tau}$ times as rows.
- τ – strength; well known to be equal to the dual distance of C minus one.
- **Definition 2.** If $C \subset H(n,2)$ is a τ-design and $y \in H(n,2)$ is fixed then the (possibly) multiset

$$A_y(C) = \{q_0(y), q_1(y), \dots, q_n(y)\},$$

where $q_k(y) = |\{x \in C : d(y,x) = k\}|$ for $k = 0, 1, \dots, n$, is called distance distribution of C with respect to y.

- **Problem 1.** Calculate all possible distance distributions of C for given length n, strength τ and cardinality $|C|$.
- **Problem 2.** Use the information from Problem 1 to construct or to prove nonexistence for the corresponding parameters.

- **Definition 3.** 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

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

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.

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

where $d = n(1-t)/2$.

- For fixed y, Definition 3 gives a system of $\tau+1$ linear equations for the distance distribution of C with respect to y.
- Delsarte (1973) – The distance distribution can be found if the design has at most $\tau+1$ different distances.
- In fact, for small cases, the distance distributions can be calculated for lager number of different distances, sometimes in all possible cases.

- The system:

$$\sum_{i=0}^{n} q_i(y) \left(1 - \frac{2i}{n}\right)^k = f_{0,k}|C|, \quad k = 0, 1, \ldots, \tau, \qquad (2)$$

where $f_{0,2m-1} = 0$, $f_{0,0} = 1$, $f_{0,2} = \frac{1}{n}$, $f_{0,4} = \frac{3n-2}{n^3}$, $f_{0,6} = \frac{15n^2-30n+16}{n^5}$ and so on.

- Usually we obtain many solutions and we try to put some order by using the Fazekas-Levenshtein bound (1997) on the covering radius of C (in terms of the strength and length).

- Problem 3. Decide if the Fazekas-Levenshtein bound can be attained. If so, classify the corresponding OA, otherwise find new bound.

- Observation – if $y = (0, 0, \ldots, 0) \notin C$, then for every $x \in C$

$$p_0(x)+p_2(x)+\cdots+p_{2[\frac{n}{2}]}(x) = \begin{cases} q_0(y) + q_2(y) + \cdots + q_{2[\frac{n}{2}]}(y) \\ q_1(y) + q_3(y) + \cdots + q_{2[\frac{n+1}{2}]-1}(y) \end{cases}$$

- For $(\tau, n) = (4, 8)$, $(5, 9)$ and $(6, 10)$ the FL bound coincides with an inner product. However the corresponding systems do not have integer solutions. Therefore the FL bound can not be attained in these cases.

- For $(\tau, n, |C|) = (5, 10, 192)$ we obtain 85 solutions for $y \notin C$, sorted as follows:
  – eleven solutions if the covering radius is 2, with $q_2(y) \in [16, 21]$;
  – seventy-four solutions if the covering radius is 1.
  and 35 solutions for $y \in C$.

We now try to rule out the solutions one by one by showing that there are no possible combinations to fit in C.

For example, it is not difficult to rule out the solutions

$q_0 = q_1 = q_4 = q_6 = q_9 = q_{10} = 0$, $q_2 = q_8 = 16$, $q_3 = 24$, $q_5 = 112$, $q_7 = 24$.

and (a symmetric one)

$q_0 = q_1 = q_9 = q_{10} = 0$, $q_2 = q_8 = 17$, $q_3 = q_7 = 18$, $q_4 = q_6 = 15$, $q_5 = 92$.

Here $y = (0, 0, \dots, 0)$ is a point where the covering radius is attained, and y is omitted in the notation of the distance distribution.