Orthogonal Arrays - Review

Silvia Boumova, Nikolai Manev

November 6, 2018

1 Introduction

Definition 1.1. *Let $\mathscr{A}$ be an alphabet of q symbols. An **Orthogonal Array** $OA(M,n,q,t)$ **of strength** t **with** M **rows,** n **columns** $(n \geq t)$**, and** q **levels** is an $M \times n$ matrix (array) with entries from $\mathscr{A}$ so that every $M \times t$ submatrix contains each of the q^t possible t-tuples equally often as a row (say λ times).*

Obviously $M = \lambda q^t$ and λ is called ***index*** of the orthogonal array.
Often used notations for $OA(M,n,q,t)$ are also $OA(M,q^n,t)$ or $t-(q,n,\lambda)$.

The origin of orthogonal arrays is experimental statistic. C. R. Rao (1946, 1947, 1949) introduced them for use in fractional factorial experiments. Since their introduction many researchers coming from different scientific arrays began to contribute to the subject. The diversity of their background has caused various terms to be used for one and the same notions in the area. Here are the most used terms for the basic parameters of $OA(M,n,q,t)$:

M**:** number of experimental runs; size; number of rows;

n**:** number of factors; constraints; columns; number of variables;

q**:** number of levels; number of symbols;

t**:** strength; estimability of parameters;

λ**:** index;

$\mathscr{A}^n$**:** full factorial design;

$OA(M,n,q,t)$**:** fractional factorial design; fraction;

Generally $OA(M,n,q,t)$ is a multi-subset of $\mathscr{A}^n$, that is, it can have repeated rows, but all its different rows form a subset of $\mathscr{A}^n$. Orthogonal area without repeated rows is called ***simple***.

$t-(q,t,\lambda)$, that is, $OA(\lambda q^t,t,q,t)$ is a trivial example of an orthogonal array: each element of $\mathscr{A}^t$ is repeated λ times.

Usually $\mathscr{A} = \mathbb{Z}_q$, the additive group of integers modulo q, or $\mathbb{C}_q$, the multiplicative group of q-roots of unity in $\mathbb{C}$. (Recall that $\mathbb{Z}_q \cong \mathbb{C}_q$.) But if q is a prime power the finite field $GF(q)$ can

be used for an alphabet, too. Such an approach enables results from coding theory to be drawn in for solving problems concerning orthogonal arrays.

Obviously, an orthogonal array of strength t is also of strength t', for any $t' < t$.

The notion orthogonal array can be generalized to so called ***mixed orthogonal array***. Let $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n$ be a set of alphabets with cardinality $q_1, q_2, \ldots, q_n$, respectively. A mixed orthogonal array is defined as a multi-subset of $\mathscr{A}_1 \times \mathscr{A}_2 \times \cdots \times \mathscr{A}_n$ satisfying the properties given in Definition 1.1.

1.1 Basic properties

Proposition 1.2. *For an $OA(M,n,q,t)$ the following properties hold*

(i) A permutation of the runs or factor in $OA(M,n,q,t)$ results in orthogonal array with the same parameters.

(ii) A permutation of the symbols of any factor in $OA(M,n,q,t)$ results in orthogonal array with the same parameters.

(iii) Any $M \times k$ sub-array of $OA(M,n,q,t)$ is an $OA(M,k,q,t')$, where $t' = \min\{t,k\}$.

(iv) If $A = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}$ is an $OA(M,n,q,t)$, where A_1 itself is an $OA(M_1,n,q,t_1)$, then A_2 is an $OA(M-M_1, n, q, t_2)$ with $t_2 \geq \min\{t,t_1\}$.

Proposition 1.3. *Existence of $OA(M,n,q,t)$ implies existence of $OA(\frac{M}{q}, n-1, q, t-1)$. Conversely, if A_i is $OA(M_i,n,q,t_i)$, $\quad i = 1,\ldots,m, \quad$ then*

$$A = \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_m \end{bmatrix}$$

is $OA(M,n,q,t)$ with $M = M_1 + M_2 + \cdots + M_m$ and strength $t \geq \min\{t_1,t_2,\ldots,t_m\}$. In partial existence of $OA(M,n,q,t)$ implies existence of $OA(qM,n+1,q,t)$.

Definition 1.4. *Two orthogonal arrays is said to be **isomorphic** if one can be obtained from the other by a sequence of permutations of its rows, columns, and the symbols of each column.*

2 The case when the alphabet is a finite field

Let the alphabet $\mathscr{A} = GF(q)$, where $q = p^e$ is a prime power. Then the set of the distinct rows of any orthogonal array $OA(M,n,q,t)$ can be considered as a q-ary code, in general nonlinear, of block length n having $\leq M$ codewords.

Definition 2.1. *An $OA(M,n,q,t)$ is said to be **linear** if it is simple and its rows form an linear space over $GF(q)$.*

If $OA(M,n,q,t)$ is linear then $M = q^k$ for some $t \le k \le n$.

Linear OAs or its translates are said to be ***regular fractions*** in statistics.

An orthogonal array whose rows form an additive group is called ***additive***. Linear OAs are additive but the converse need not hold. Alphabet of an additive OA need not to be a field, it is sufficiently to be an additive group.

Theorem 2.2. *Let R be a ring with unity, $|R| = q$. If A is an $OA(M,n,q,t)$ with entries from R, then any t columns of A are linearly independent over R.*

Proof. Let $\mathbf{v}_1,\dots,\mathbf{v}_t$ be any t columns of A, and suppose that $c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_t\mathbf{v}_t$ is the zero column. Since A has a row with 1 in $\mathbf{v}_1$ and zeros in other $t-1$ columns $\mathbf{v}_j$ it follows $c_1 = 0$. The similar arguments give $c_2 = \cdots = c_t = 0$. □

Theorem 2.3. *Let A be a $M \times n$ matrix whose rows form a linear subspace of $\mathbb{F}^n$, $\mathbb{F} = GF(q)$. If any t columns of A are linearly independent over $\mathbb{F}$, then A is an $OA(M,n,q,t)$.*

Proof. Suppose $M = q^k$, $t \le k \le n$. Let $\mathbf{G}$ be $k \times n$ submatrix of A with rank k. Then any row of A can be presented as $\mathbf{uG}$, where $\mathbf{u} \in \mathbb{F}^k$. Choose t columns of A and let $\mathbf{G}_1$ be the $k \times t$ submatrix of $\mathbf{G}$ corresponding to the chosen columns. Obviously $\operatorname{rank}\mathbf{G}_1 = t$. Hence the restriction of rows of A to the chosen columns are linear combinations of the rows of $\mathbf{G}_1$ and any t-tuple is repeated q^{k-t} times. □

Theorem 2.4. *If C is an $[n,k,d]$ q-ary code then its dual code $C^\perp$ is $OA(q^{n-k},n,q,d-1)$ with index $\lambda = q^{n-k-d+1}$. The code C itself is an $OA(q^k,n,q,d^\perp-1)$, where $d^\perp$ is the minimal distance of $C^\perp$.*

Example 2.1. Let C be the $[4,2,3]_3$ Hemming code over $\mathbb{Z}_3$ given by a parity check matrix $\mathbf{H} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix}$. The dual code $C^\perp$ is a $[4,2,3]_3$ code generated by the rows of $\mathbf{H}$. Below $C^\perp$ and its translate by 1111 are given

0	0	0	0
0	1	1	1
0	2	2	2
1	0	1	2
2	0	2	1
1	1	2	0
2	2	1	0
1	2	0	1
2	1	0	2

1	1	1	1
1	2	2	2
1	0	0	0
2	1	2	0
0	1	0	2
2	2	0	1
0	0	2	1
2	0	1	2
0	2	1	0

It is easy to check that they both are $OA(9,4,3,2)$. Indeed C is self dual, that is, $C = C^\perp$.

3 Bounds

Definition 3.1. *Let* $t \geq 2,\ q \geq 2,\ M = \lambda q^t$.

$$f(M,q,t) \stackrel{def}{=} \max\ n : \text{there exists}\ \ OA(M,n,q,t),\ i.e.,\ t-(q,n,\lambda).$$

Definition 3.2. *Let* $n \geq t \geq 2,\ q \geq 2$.

$$F(n,q,t) \stackrel{def}{=} \min\ M : \text{there exists}\ \ OA(M,n,q,t),\ i.e.,\ t-(q,n,M/q^t).$$

The following relationships between $f(M,q,t)$ and $F(n,q,t)$ hold:

$$\begin{aligned} F(n,q,t) &= \min\{M \mid f(M,q,t) \geq n\} \\ f(M,q,t) &\leq \max\{n \mid F(n,q,t) \leq M\} \end{aligned}$$

Definition 3.3.

$$A_q(n,d) \stackrel{def}{=} \{\max\ M \mid \text{an } (n,M,d)_q \text{ code exists}\}$$

3.1 Rao's bound

The following theorem gives a lower bound for $F(n,q,t)$.

Theorem 3.4 (Rao's Inequalities)**.** *For parameters of any* $OA(M,n,q,t)$ *the following inequalities hold*

$$M \geq \begin{cases} \displaystyle\sum_{i=0}^{u} \binom{n}{i}(q-1)^i, & if \quad t = 2u \\ \displaystyle\sum_{i=0}^{u} \binom{n}{i}(q-1)^i + \binom{n-1}{u}(q-1)^{u+1}, & if \quad t = 2u+1 \end{cases}$$

3.2 Krawtchouk polynomials

Definition 3.5. ***Krawtchouk polynomial*** *is a polynomial defined by*

$$K_k(x;n,q) = \sum_{j=0}^{k} (-1)^j \binom{x}{j}\binom{n-x}{k-j}(q-1)^{k-j}, \quad k = 0,1\ldots n.$$

Usually n and q have already been fixed or their values are known from context. Hence for simplicity n and q are omitted and we write only $K_k(x)$.

$K_k(x)$ is a polynomial of degree k in x with leading coefficient $(-q)^k/k!$. Here are the first two polynomials:

$$K_0(x) = 1; \qquad K_1(x) = -qx + n(q-1).$$

The generating function of Krawtchouk polynomials is

$$\sum_{k=0}^{\infty} K_k(x;n,q)z^k = (1+(q-1)z)^{n-x}(1-z)^x. \tag{1}$$

Differentiating the both sides of (1) and multiplying the result by $(1+(q-1)z)(1-z)$ one can obtain the recurrence relation

$$kK_k(t) = (-qt+(n-k+1)(q-1)+k-1)K_{k-1}(t) - (q-1)(n-k+2)K_{k-2}(t), \tag{2}$$

which holds for $k = 2,3,\ldots,n$.

In the sequel we will often use the matrices

$$\mathbf{V} = (K_i(j)),\ i,j = 1,2,\ldots,n; \qquad \mathbf{B} = (K_1(0),K_2(0),\ldots,K_n(0)).$$

It is easy to check that

$$K_k(0) = \binom{n}{k}(q-1)^k, \quad K_k(n) = (-1)^k\binom{n}{k}, \quad K_n(i) = (-1)^i(q-1)^{n-i} \tag{3}$$

Matrix $\mathbf{V}$ can be computed using the following recurrence

$$K_k(j) = K_k(j-1) - [K_{k-1}(j-1) + (q-1)K_{k-1}(j)] \qquad k,j = 1,2,\ldots,n. \tag{4}$$

It can be easily proved by replacing t by $t-1$ in (1). ($\mathbf{V}$ and $\mathbf{B}$ can be computed by Matlab function [V,B]=kravalrec(n,q) realized in kravalrec.m)

Krawtchouk polynomials satisfy many relations. Here are several of them

$$(q-1)^i\binom{n}{i}K_k(i) = (q-1)^k\binom{n}{k}K_i(k);$$

$$K_k(t;n) = (q-1)K_{k-1}(t;n-1) + K_k(t;n-1);$$

$$(q-1)K_k(t;n) + K_k(t-1;n) = qK_k(t-1;n-1);$$

$$\sum_{k=0}^{n}\binom{n-k}{n-j}K_k(t) = q^j\binom{n-t}{j};$$

$$\sum_{k=0}^{m}K_k(t;n) = K_m(t-1;n-1);$$

The next two relations are known as ***orthogonality relations***.

$$\sum_{i=0}^{n}\binom{n}{i}(q-1)^iK_k(i)K_l(i) = \delta_{kl}\binom{n}{k}(q-1)^kq^n \tag{5}$$

$$\sum_{i=0}^{n}K_k(i)K_i(l) = \delta_{kl}q^n \tag{6}$$

For any polynomial $f(x)$ of degree $m \le n$ there is a unique expansion

$$f(x) = \sum_{k=0}^{m} f_k K_k(x),$$

which is called the Krawtchouk expansion of $f(x)$. The coefficients are given by

$$f_k = \frac{1}{q^n} \sum_{i=0}^{n} f(i) K_i(k).$$

An useful unknown fact

Matrix $\mathbf{V}$ is a product of two triangle and one diagonal matrices, exactly $\mathbf{V} = \mathbf{PDQ}$, where

$$\mathbf{P} = (p_{ki}) = \left((-1)^k \binom{i}{k} \right); \qquad \mathbf{Q} = (q_{ij}) = \left((-1)^{i-j} \binom{n-j}{n-i} (q-1)^{i-j} \right).$$

and $\mathbf{D} = \mathbf{diag}(q^{n-1}, \ldots, q, 1)$ (Matlab functions *P=pmat(n)* and *Q=qmat(n,q)* realized by pmat.m and qmat.m, respectevely, give matrices.)

$\mathbf{P}$ is an idempotent matrix, that is, $\mathbf{P}^{-1} = \mathbf{P}$, while $\mathbf{Q}^{-1}$ is absolute value of $\mathbf{Q}$:

$$\mathbf{Q}^{-1} = \left(\binom{n-j}{n-i} (q-1)^{i-j} \right).$$

The proof of both statement is based on the following relation:

$$\sum_{j=k}^{m} (-1)^{j-k} \binom{m}{j} \binom{j}{k} = \delta_{km}$$

(The Matlab file qqmat.m realizes the function that compute $\mathbf{Q}^{-1}\mathbf{D}^{-1}$.)

Example 3.1. In the case $n = 4,\ q = 3$ we have $\mathbf{V}$ is equal to

$$\mathbf{V} = \begin{pmatrix} 5 & 2 & -1 & -4 \\ 6 & -3 & -3 & 6 \\ -4 & -4 & 5 & -4 \\ -8 & 4 & -2 & 1 \end{pmatrix} = \begin{pmatrix} -1 & -2 & -3 & -4 \\ 0 & 1 & 3 & 6 \\ 0 & 0 & -1 & -4 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 27 & 0 & 0 & 0 \\ 0 & 9 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ -6 & 1 & 0 & 0 \\ 12 & -4 & 1 & 0 \\ -8 & 4 & -2 & 1 \end{pmatrix}$$

$$\mathbf{Q}^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 6 & 1 & 0 & 0 \\ 12 & 4 & 1 & 0 \\ 8 & 4 & 2 & 1 \end{pmatrix}$$

Normalized Krawtchouk polynomials

Let

$$t_i = 1 - \frac{2i}{n},\ i = 0, 1, \ldots, n. \tag{7}$$

Hence $1 = t_0 > t_1 > \cdots > t_n = -1$ and $t_i = -t_{n-i}$.

Definition 3.6. *Normalized Krawtchouk polynomials are defined by*

$$Q_k(t) \stackrel{def}{=} \frac{1}{K_k(0)} K_k\left(\frac{n}{2}(1-t)\right) = \frac{1}{\binom{n}{k}(q-1)^k} K_k\left(\frac{n}{2}(1-t)\right).$$

A straightforward computations show that $Q_k(1) = 1$ and

$$K_k(i) = \binom{n}{k}(q-1)^k Q_k(t_i), i = 0, 1, \ldots, n. \tag{8}$$

Replacing $K_k(i)$ in the orthogonality relations (5) and (6) we obtain respectively

$$\sum_{i=0}^{n} \binom{n}{i}(q-1)^i Q_k(t_i) Q_l(t_i) = \frac{q^n}{\binom{n}{k}(q-1)^k}\delta_{kl} \tag{9}$$

$$\sum_{i=0}^{n} \binom{n}{i}(q-1)^i Q_k(t_i) Q_i(t_l) = \frac{q^n}{\binom{n}{k}(q-1)^k}\delta_{kl} \tag{10}$$

(9), (10), and $Q_0(t) = 1$ give

$$\sum_{i=0}^{n} \binom{n}{i}(q-1)^i Q_k(t_i) = \sum_{i=0}^{n} \binom{n}{i}(q-1)^i Q_i(t_k) = \begin{cases} 0, & k > 0 \\ q^n, & k = 0 \end{cases} \tag{11}$$

The equality (9) shows that the polynomials $\{Q_k(t)\}$ are orthogonal polynomials in respect to the inner product defined by

$$< f(t), g(t) > \stackrel{def}{=} \frac{1}{q^n} \sum_{i=0}^{n} \binom{n}{i}(q-1)^i f(t_i) g(t_i). \tag{12}$$

Hence any polynomial $f(x)$ of degree $m \leq n$ has a unique expansion

$$f(x) = \sum_{k=0}^{m} f_k Q_k(x),$$

in the orthogonal basis $\{Q_k(t)\}$. Using the orthogonality relation (9) we can obtain

Theorem 3.7.

$$f_k = \frac{\binom{n}{k}(q-1)^k}{q^n} \sum_{i=0}^{n} \binom{n}{i}(q-1)^i f(t_i) Q_k(t_i), \quad k = 0, 1, \ldots, n. \tag{13}$$

Proof. Let $f(t) = f_0 + f_1Q_1(t) + \cdots + f_mQ_m(t)$. Then for any $i = 0, 1, \ldots, n$

$$f(t_i) = f_0 + f_1Q_1(t_i) + \cdots + f_jQ_j(t_i) + \cdots + f_mQ_m(t)$$

Multiplying the above $n+1$ equalities, respectively by $\binom{n}{i}(q-1)^iQ_k(t_i),\ i = 0, 1, \ldots, n$ and summarizing we obtain

$$\sum_{i=0}^{n}\binom{n}{i}(q-1)^i f(t_i)Q_k(t_i) = \sum_{j=0}^{m}\left(f_j\sum_{i=0}^{n}\binom{n}{i}(q-1)^iQ_j(t_i)Q_k(t_i)\right)$$

But the orthogonality of polynomials, i.e., (9) shows that

$$\sum_{i=0}^{n}\binom{n}{i}(q-1)^i f(t_i)Q_k(t_i) = f_k\frac{q^n}{\binom{n}{k}(q-1)^k}.$$

□

Let b_k denote the first coefficient in the Q-expansion of t^k, that is, $t^k = b_k + \sum_{j=1}^{k} a_jQ_j(t)$. Using (13) and $Q_0(t) = 1$ we obtain

Corollary 3.8.

$$b_k = \frac{1}{q^n}\sum_{i=0}^{n}\binom{n}{i}(q-1)^i t_i^k, \quad k = 0, 1, \ldots, n. \tag{14}$$

In partial

$$b_0 = 1, \quad b_1 = \frac{2-q}{q}, \quad b_2 = 1 - \frac{4(n-1)(q-1)}{nq^2}.$$

3.3 Linear programming bound (LPB)

Let $\chi_a : \mathbb{Z}_q \to \mathbb{C}_q$ be an additive character of $\mathbb{Z}_q$ defined by $\chi_a(x) = \xi^{ax}$, where ξ is a primitive q-root of unity, $a, x \in \mathbb{Z}_q$. Recall that additive character is a homomorphism of an additive group into $\mathbb{C}^*$. It is easy to check that

$$\chi_0(x) = \chi_a(0) = 1, \quad \chi_a(x) = \chi_x(a), \quad \chi_a(x+y) = \chi_a(x)\chi_a(y), \quad \chi_a(-x) = \chi_a(x)^{-1} = \overline{\chi_a(x)}$$

$$\sum_{x\in\mathbb{Z}_q}\chi_a(x) = \begin{cases} 0, & a \neq 0 \\ q, & a = 0 \end{cases}, \qquad \text{or equivalently} \qquad \sum_{x\in\mathbb{Z}_q^*}\chi_a(x) = \begin{cases} -1, & a \neq 0 \\ q-1, & a = 0 \end{cases}. \tag{15}$$

Let us now for any $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{Z}_q^n$ define an additive character $\chi_{\mathbf{u}} : \mathbb{Z}_q^n \to \mathbb{C}_q$ by

$$\chi_{\mathbf{u}}(\mathbf{v}) = \xi^{<\mathbf{u},\mathbf{v}>} = \prod_{i=1}^{n}\chi_{u_i}(v_i)$$

The following properties are straightforward

$$\chi_{\mathbf{0}}(\mathbf{u}) = \chi_{\mathbf{u}}(\mathbf{0}) = 1, \quad \chi_{\mathbf{u}}(\mathbf{v}) = \chi_{\mathbf{v}}(\mathbf{u}), \quad \chi_{\mathbf{u}}(\mathbf{v}+\mathbf{w}) = \chi_{\mathbf{u}}(\mathbf{v})\chi_{\mathbf{u}}(\mathbf{w}) \quad \chi_{\mathbf{u}}(-\mathbf{v}) = \chi_{-\mathbf{u}}(\mathbf{v}) = \overline{\chi_{\mathbf{u}}(\mathbf{v})}$$

Proposition 3.9. *For any* $\mathbf{u} \in \mathbb{Z}_q^n$

$$\sum_{\mathbf{v}\in\mathbb{Z}_q^n} \chi_{\mathbf{u}}(\mathbf{v}) = \begin{cases} 0, & \mathbf{u} \neq \mathbf{0} \\ q^n, & \mathbf{u} = \mathbf{0} \end{cases}$$

Proof. Let $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$.

$$\begin{aligned} \sum_{\mathbf{v}\in\mathbb{Z}_q^n} \chi_{\mathbf{u}}(\mathbf{v}) &= \sum_{\mathbf{v}\in\mathbb{Z}_q^n} \prod_{i=1}^{n} \chi_{u_i}(v_i) = \sum_{(v_1,\ldots,v_{n-1})\in\mathbb{Z}_q^{n-1}} \prod_{i=1}^{n-1} \chi_{u_i}(v_i) \left(\sum_{v_n\in\mathbb{Z}_q} \chi_{u_n}(v_n) \right) = \cdots \\ &= \left(\sum_{v\in\mathbb{Z}_q} \chi_{u_1}(v) \right) \left(\sum_{v\in\mathbb{Z}_q} \chi_{u_2}(v) \right) \cdots \left(\sum_{v\in\mathbb{Z}_q} \chi_{u_n}(v) \right) \end{aligned}$$

According to (15) if there is $u_i \neq 0$ then the i-th factor is zero, thus the product is zero. Otherwise all factors are equal to q, hence, the product is q^n. □

Lemma 3.10. *Let* $\mathbf{u} \in \mathbb{Z}_q^n$ *be a fixed vector of weight* $wt(\mathbf{u}) = t$ *and* $W_k \subset \mathbb{Z}_q^n$ *be the subset of all vectors of weight k. Then*

$$\sum_{\mathbf{v}\in W_k} \chi_{\mathbf{u}}(\mathbf{v}) = K_k(wt(\mathbf{u})).$$

Proof. Let $wt(\mathbf{u}) = t$ and for simplicity of notations let $\mathbf{u} = (u_1, \ldots, u_t, 0, \ldots, 0)$, $u_i \neq 0$. Choose k positions $h_1, h_2, \ldots, h_k$ and let $0 < h_1 < h_2 < \cdots < h_j \leq t < h_{j+1} < \cdots < h_k \leq n$. Denote by $D_j \subset W_k$ the set of all vectors of weight k whose nonzero coordinates are $h_1, \ldots, h_k$. Obviously there are $\binom{t}{j}\binom{n-t}{k-j}$ choices for D_j. Now let us evaluate the sum

$$\begin{aligned} \sum_{\mathbf{v}\in D_j} \chi_{\mathbf{u}}(\mathbf{v}) &= \sum_{\mathbf{v}\in D_j} \chi_{u_{h_1}}(v_{h_1}) \cdots \chi_{u_{h_j}}(v_{h_j}) \chi_0(v_{h_{j+1}}) \cdots \chi_0(v_{h_k}) \\ &= \left(\sum_{v\in\mathbb{Z}_q^*} \chi_{u_{h_1}}(v) \right) \cdots \left(\sum_{v\in\mathbb{Z}_q^*} \chi_{u_{h_j}}(v) \right) \left(\sum_{v\in\mathbb{Z}_q^*} \chi_0(v) \right) \cdots \left(\sum_{v\in\mathbb{Z}_q^*} \chi_0(v) \right) \end{aligned}$$

Now applying (15) we get

$$\sum_{\mathbf{v}\in D_j} \chi_{\mathbf{u}}(\mathbf{v}) = (-1)^j (q-1)^{k-j}$$

Therefore,

$$\sum_{\mathbf{v}\in W_k} \chi_{\mathbf{u}}(\mathbf{v}) = \sum_{j=0}^{k} (-1)^j \binom{t}{j} \binom{n-t}{k-j} (q-1)^{k-j} = K_k(t).$$

□

Let C be $(n, M)_q$ code, that is, C is a subset of $\mathbb{Z}_q^n$ having M vectors.

Definition 3.11. *The sequence* $\{A_i\}$, $i = 0, 1, \ldots, n$ *defined by*

$$A_i \stackrel{def}{=} \frac{1}{M} \left| \{(\mathbf{x}, \mathbf{y}) \in C^2 \mid \operatorname{dist}(\mathbf{x}, \mathbf{y}) = i\} \right|$$

is called ***distance distribution*** *of C.*

When C is a linear code then the distance distribution coincides with weight distribution and A_i are nonnegative integers.

Example 3.3?. Let $n = 3$, $q = 3$ and $C = \{000, 101, 220\}$. Then

$$A_0 = \frac{3}{3} = 1, \quad A_1 = 0, \quad A_2 = \frac{4}{3}, \quad A_3 = \frac{2}{3}.$$

Lemma 3.12. *Let $\{A_i\}$, $i = 0, 1, \ldots, n$ be distance distribution of an $(n, M)_q$ code C over $\mathbb{Z}_q$. Then*

$$\sum_{i=0}^{n} A_i K_k(i) \geq 0$$

for any $k = 0, 1, \ldots, n$.

Proof. For any vector $\mathbf{z} \in \mathbb{Z}_q^n$ we have

$$0 \leq \left| \sum_{\mathbf{x} \in C} \chi_{\mathbf{x}}(\mathbf{z}) \right|^2 = \left(\sum_{\mathbf{x} \in C} \chi_{\mathbf{x}}(\mathbf{z}) \right) \left(\sum_{\mathbf{x} \in C} \overline{\chi_{\mathbf{x}}(\mathbf{z})} \right) = \left(\sum_{\mathbf{x} \in C} \chi_{\mathbf{x}}(\mathbf{z}) \right) \left(\sum_{\mathbf{y} \in C} \chi_{-\mathbf{y}}(\mathbf{z}) \right)$$

$$= \sum_{(\mathbf{x},\mathbf{y}) \in C^2} \chi_{\mathbf{x}}(\mathbf{z}) \chi_{-\mathbf{y}}(\mathbf{z}) = \sum_{(\mathbf{x},\mathbf{y}) \in C^2} \chi_{\mathbf{x}-\mathbf{y}}(\mathbf{z}) = \sum_{i=0}^{n} \sum_{\substack{(\mathbf{x},\mathbf{y}) \in C^2 \\ wt(\mathbf{x}-\mathbf{y}) = i}} \chi_{\mathbf{x}-\mathbf{y}}(\mathbf{z})$$

Summarizing on $\mathbf{z}$ with $wt(\mathbf{z}) = k$ we obtain

$$0 \leq \sum_{\mathbf{z} \in W_k} \left| \sum_{\mathbf{x} \in C} \chi_{\mathbf{x}}(\mathbf{z}) \right|^2 = \sum_{i=0}^{n} \sum_{\substack{(\mathbf{x},\mathbf{y}) \in C^2 \\ wt(\mathbf{x}-\mathbf{y}) = i}} \sum_{\mathbf{z} \in W_k} \chi_{\mathbf{x}-\mathbf{y}}(\mathbf{z}) = \sum_{i=0}^{n} M A_i K_k(i).$$

□

Remark. The aforesaid results hold also for a finite field with $q = p^e$ elements. In that case characters are defined as homomorphism into $\mathbb{C}_p$, i.e., they are powers of p-th root of unity.

Definition 3.13.

$$A_q(n, d) \stackrel{def}{=} \max\{M \mid an\ (n, M, d)_q \quad q - ary\ code\ exists\}$$

Theorem 3.14 (LPB for codes)**.** *Let $n, q \geq 2, d \in \mathbb{N}$. Then*

$$A_q(n, d) \leq \max \sum_{i=0}^{n} A_i,$$

where A_i, $i = 0, 1, \ldots, n$ satisfy the constrains

$$\begin{aligned} A_i \geq 0, \quad A_0 &= 1, \\ A_i &= 0, \qquad for\ i = 1, \ldots, d-1 \\ \sum_{i=0}^{n} A_i K_k(i) &\geq 0 \qquad for\ k = 0, 1, \ldots, n \end{aligned}$$

Proof. By Lemma 3.12 the distance distribution of any $(n,M,d)_q$ code C satisfy the constrains given in the theorem. Furthermore $\sum_{i=0}^{n} A_i = M^{-1}|C^2| = M$. □

Example 3.?. Now we will prove that $A_3(4,3) = 9$. According to the Theorem 3.14 we have to maximize $1 + A_3 + A_4$ with constrains

$$A_3, A_4 \geq 0, \qquad K_k(0) + A_3 K_k(3) + A_4 K_k(4) \geq 0, \quad k = 1,2,3,4.$$

The values of $K_k(j)$ for $n = 4$ and $q = 3$ are given in Example 3.1. Hence

$$\begin{aligned} -A_3 - 4A_4 &\geq -8 \\ -3A_3 + 6A_4 &\geq -24 \\ 5A_3 - 4A_4 &\geq -32 \\ -2A_3 + 6A_4 &\geq -16 \end{aligned}$$

Using a software for solving linear programming problems, for example *linprog* of Matlab, we obtain $A_3 = 8,\ A_4 = 0$ and $A_3(4,3) \leq 9$. On the other hand the $[4,2,3]_3$ Hemming code over $\mathbb{Z}_3$ has 9 codewords. Thus $A_3(4,3) = 9$. (The command of Matlab is

```
[Y,fval,exitflag]=linprog([-1 -1],A,[8; 24; 32; 16],[],[],lb),
```

where lb=[0;0] and A=[1 4; 3 -6; -5 4; 2 -1].)

Theorem 3.15 (Dual LPB for codes)**.** *If there exists a polynomial*

$$f(x) = 1 + f_1 K_1(x) + f_2 K_2(x) + \cdots + f_n K_n(x),$$

such that the following conditions hold:

$$\begin{aligned} f_k &\geq 0, \qquad \text{for } k = 1,2,\ldots,n \\ f(j) &\leq 0, \qquad \text{for } j = d, d+1, \ldots, n \end{aligned} \tag{16}$$

then

$$A_q(n,d) \leq f(0).$$

Proof. Suppose $A_0, A_1, \ldots, A_n$ satisfy the conditions of Theorem 3.14, i.e. $A_0 = 1,\ A_1 = \cdots = A_{d-1} = 0,\ A_i \geq 0$ for $i = d, \ldots, n$, and for $k = 0, 1, \ldots, n$

$$K_k(0) + \sum_{i=d}^{n} A_i K_k(i) \geq 0.$$

Multiplying the above inequalities by $f_k \geq 0$ and summarizing them for $k = 1, \ldots, n$ we obtain

$$f(0) - 1 + \sum_{i=d}^{n} A_i (f(i) - 1) \geq 0, \qquad \text{thus} \qquad f(0) + \sum_{i=d}^{n} A_i f(i) \geq 1 + \sum_{i=d}^{n} A_i.$$

But according to the conditions of the theorem $A_i f(i) \leq 0$. Hence $f(0) \geq 1 + \sum_{i=d}^{n} A_i$. □

The advantage of the dual LPB bound is that any polynomial satisfying the conditions of the theorem, not only optimal solution of the corresponding linear programming problem, gives bound for $A_q(n,d)$. This fact enables theoretical bounds to be derived.

Example 3.?. Let $n=5$, $q=3$, $d=3$. We want to evaluate $A_3(5,3)$. We will do this by solving the linear programming problem corresponding to Theorem 3.15 for considered parameters. An alternative approach is described below. For $n=5$, $q=3$ we compute that

$$\mathbf{V}=(K_k(j))=\begin{pmatrix} 7 & 4 & 1 & -2 & -5 \\ 16 & 1 & -5 & -2 & 10 \\ 8 & -10 & -1 & 8 & -10 \\ -16 & -4 & 8 & -7 & 5 \\ -16 & 8 & -4 & 2 & 1 \end{pmatrix} \qquad \text{and} \qquad B=(K_k(0))=(10,40,80,80,32)$$

We have to minimize $10f_1+40f_2+80f_3+80f_4+32f_5$ under constrains $f_i\geq 0$ and

$$(f_1,\ldots,f_5)\mathbf{V}(:,3:5)=(f_1,\ldots,f_5)\begin{pmatrix} 1 & -2 & -5 \\ -5 & -2 & 10 \\ -1 & 8 & -10 \\ 8 & -7 & 5 \\ -4 & 2 & 1 \end{pmatrix}\leq\begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}$$

The Matlab command

```
[x,fmin]=linprog(B,V(:,3:5)', -ones(3,1),[],[],zeros(5,1)),
```

gives fmin=17 and x=$(1/2,1/6,0,0,1/6)$. Hence

$$f(x)=1+\frac{1}{2}K_1(x)+\frac{1}{6}K_2(x)+\frac{1}{6}K_5(x), \qquad A_3(5,3)\leq f(0)=18.$$

An alternative usage of dual LPB for codes

We can apply this approach when we have problems to find an optimal solution by the approach described in the above example.

The inequalities $f(j)\leq 0$ imply

$$f_1K_1(j)+f_2K_2(j)+\cdots+f_nK_n(j)\leq -1, \quad j=d,d+1,\ldots,n$$

Suppose we have only equalities. Then we have to minimize $f(0)$ under condition

$$(f_1,f_2,\ldots,f_n)\mathbf{V}_d=(-1,-1,\ldots,-1), \tag{17}$$

where the $n\times(n-d+1)$ matrix $\mathbf{V}_d$ is obtained by deleting the first $d-1$ columns of $\mathbf{V}$.

Let $\mathbf{P}_d=\mathbf{P}(d:n,d:n)$, $\mathbf{D}_d$, and $\mathbf{Q}_d=\mathbf{Q}^{-1}(d:n,d:n)$ be the matrices obtained by deleting the first $d-1$ rows and columns of $\mathbf{P}$, $\mathbf{D}^{-1}$, and $\mathbf{Q}^{-1}$, respectively. Multiplying both sides of (17) from the right we obtain

$$(f_1,f_2,\ldots,f_n)\mathbf{W}_d=(g_1,g_2,\ldots,g_{n-d+1})=\mathbf{g}, \tag{18}$$

where

$$\mathbf{W}_d = \begin{pmatrix} \mathbf{U} \\ \mathbf{I} \end{pmatrix}, \qquad \mathbf{U} \text{ is } (d-1)\times(n-d+1) \text{ matrix}, \quad \mathbf{I} \text{ is } (n-d+1)\times(n-d+1) \text{ unity matrix}.$$

The general solution of the obtained linear system (18) is

$$f_1 = t_1, \ldots, f_{d-1} = t_{d-1} \qquad (f_d, \ldots, f_n) = \mathbf{g} - (t_1, \ldots, t_{d-1})\mathbf{U},$$

where $t_1, \ldots, t_{d-1}$ are parameters.

Hence we reduced our problem to a minimization of

$$f(0) = 1 + (K_d(0), \ldots, K_n(0))\mathbf{g}^\tau + [(K_1(0), \ldots, K_{d-1}(0))\mathbf{I} - (K_d(0), \ldots, K_n(0))\mathbf{U}^\tau](t_1, \ldots, t_{d-1})^\tau$$

depending on $d-1$ nonnegative variables t_i that satisfy $n-d+1$ linear constrains.

Note that any alternation of the vector $(-1,-1,\ldots,-1)$ implies an alternation only in $\mathbf{g}$ and its new value can be easily computed. This fact facilitates minimization of $f(0)$.

Example 3.2. Let $n = 5$, $q = 3$, $d = 3$. We want to evaluate $A_3(5,3)$.
The matrices $\mathbf{V}_d$ and B are

$$\mathbf{V}_d = \begin{pmatrix} 1 & -2 & -5 \\ -5 & -2 & 10 \\ -1 & 8 & -10 \\ 8 & -7 & 5 \\ -4 & 2 & 1 \end{pmatrix}, \qquad \mathbf{B} = \begin{pmatrix} 10 \\ 40 \\ 80 \\ 80 \\ 32 \end{pmatrix}, \quad \mathbf{P}_d = \begin{pmatrix} -1 & -4 & -10 \\ 0 & 1 & 5 \\ 0 & 0 & -1 \end{pmatrix}, \quad \mathbf{Q}_d = \begin{pmatrix} 1 & 0 & 0 \\ 4 & 1 & 0 \\ 4 & 2 & 1 \end{pmatrix}$$

$$\mathbf{W}_d = \begin{pmatrix} 3 & 8 & 15 \\ -3 & -6 & -10 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \mathbf{g} = (1,3,6).$$

Hence,

$$f_1 = u \geq 0,\ f_2 = v \geq 0,\ f_3 = 1 - 3u + 3v \geq 0,\ f_4 = 3 - 8u + 6v, \geq 0\ f_5 = 6 - 15u + 10v \geq 0$$

$$f(0) = 513 - 1350u + 1080v = 27(19 - 50u + 40v).$$

The "critical point"(verteces) are (0,0), (1/3,0), (1/2,1/6), (3/5,3/10). Simple computation show that $\min f(0) = 18$ obtained in the point (1/2,1/6).

Therefore $A_3(5,3) \leq 18$.

Linear programming bound for orthogonal arrays

Lemma 3.16. *An $(n,M)_q$ code C over $\mathbb{Z}_q$ is an $OA(n,M,q,t)$ if and only if*

$$\sum_{\mathbf{v}\in C} \chi_{\mathbf{u}}(\mathbf{v}) = 0,$$

for any $\mathbf{u} \in \mathbb{Z}_q^n$ of weight $1 \leq \mathrm{wt}(\mathbf{u}) \leq t$.

Proof. Necessity. If C is $OA(n,M,q,t)$ and $\mathbf{u} \in \mathbb{Z}_q^n$ of weight $wt(\mathbf{u}) = t$, then $\sum_{\mathbf{v}\in C} \chi_{\mathbf{u}}(\mathbf{v})$ is M/q^t times the sum $\sum_{\mathbf{v}\in\mathbb{Z}_q^t} \chi_{\mathbf{u}}(\mathbf{v}) = 0$ by Proposition 3.9.
Sufficiency. Let us fix t columns and $k(i_1,\ldots,i_t)$ be the number of occurrences of the t-tuple $(i_1,\ldots,i_t)$ as a row inn the considered t columns. The sum of all $k(i_1,\ldots,i_t)$ is M. For any nonzero t-tuple $\mathbf{u}$ having $(u_1,\ldots,u_t)$ in the chosen t columns and zero elsewhere the sum $\sum_{\mathbf{v}\in C} \chi_{\mathbf{u}}(\mathbf{v}) = 0$. Also $\chi_{\mathbf{u}}(\mathbf{v})$ occurs $k(i_1,\ldots,i_t)$ times for $\mathbf{v}$ having $(i_1,\ldots,i_t)$ in the considered columns and zero elsewhere. Hence we obtain a linear system of q^t unknowns $k(i_1,\ldots,i_t)$ and q^t equations. The matrix of the system is the table of characters, thus its determinant is nonzero. Therefore the system has unique solution. But $k(i_1,\ldots,i_t) = M/q^t$ for any t-tuples is an obvious solution.

Remark. For example, in the case $q = 3$, $t = 2$ the matrix of the system is

$$\begin{array}{ccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & \omega & \omega^2 & 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\
1 & \omega^2 & \omega & 1 & \omega^2 & \omega & 1 & \omega^2 & \omega \\
1 & 1 & 1 & \omega & \omega & \omega & \omega^2 & \omega^2 & \omega^2 \\
1 & \omega & \omega^2 & \omega & \omega^2 & 1 & \omega^2 & 1 & \omega \\
1 & \omega^2 & \omega & \omega & 1 & \omega^2 & \omega^2 & \omega & 1 \\
1 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega & \omega & \omega \\
1 & \omega & \omega^2 & \omega^2 & 1 & \omega & \omega & \omega^2 & 1 \\
1 & \omega^2 & \omega & \omega^2 & \omega & 1 & \omega & 1 & \omega^2
\end{array}$$

where $\omega^3 = 1$. □

Theorem 3.17 (LPB for orthogonal arrays)**.** *Let $n,q \geq 2, t \in \mathbb{N}$. Then*

$$F(n,q,t) \geq \min \sum_{i=0}^{n} A_i,$$

where A_i, $i = 0,1,\ldots,n$ satisfy the constrains

$$\begin{aligned}
&A_i \geq 0, \quad A_0 \geq 1, \\
&\sum_{i=0}^{n} A_i K_k(i) \geq 0 \qquad \text{for } k = 0,1,\ldots,n \\
&\sum_{i=0}^{n} A_i K_k(i) = 0 \qquad \text{for } k = 1,\ldots,t
\end{aligned}$$

Proof. Let C be $(n,M)_q$ code over $\mathbb{Z}_q$ whose distance distribution $\{A_i\}$ satisfies the condition of the theorem. Then the proof of Lemma 3.12 shows that $\sum_{i=0}^{n} A_i K_k(i) = 0$ implies

$$\left| \sum_{\mathbf{x}\in C} \chi_{\mathbf{x}}(\mathbf{z}) \right|^2 = 0 \qquad \text{thus} \qquad \sum_{\mathbf{x}\in C} \chi_{\mathbf{z}}(\mathbf{x}) = \sum_{\mathbf{x}\in C} \chi_{\mathbf{x}}(\mathbf{z}) = 0$$

for any $\mathbf{z} \in \mathbb{Z}_q^n$ of weight $1 \leq \mathrm{wt}(\mathbf{z}) \leq t$. Now Lemma 3.16 gives that C (if there exists) is an $OA(n,M,q,t)$ with distance distribution $\{A_i\}$. □

Example 3.?. Let us determine $F(4,3,2)$. The Hamming $[4,2,3]_3$ code (it is self-dual) is $OA(9,4,3,2)$. ($A_0 = 1, A_3 = 8, A_1 = A_2 = A_4 = 0$) Hence $F(4,3,2) \le 9$. Now using the LPB we will find a lower bound for $F(4,3,2)$.

We have to solve the following linear programming problem: Find $\min(A_1 + \cdots + A_4)$

$$\begin{pmatrix} 5 & 2 & -1 & -4 \\ 6 & -3 & -3 & 6 \end{pmatrix} \begin{pmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \end{pmatrix} = \begin{pmatrix} -8 \\ -24 \end{pmatrix} \qquad \begin{pmatrix} -4 & -4 & 5 & -4 \\ -8 & 4 & -2 & 1 \end{pmatrix} \begin{pmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \end{pmatrix} \ge \begin{pmatrix} -32 \\ -16 \end{pmatrix}$$

Using function *linprog* of Matlab we obtain solution $(0,0,8,0)$ and $\min = 8$. Hence $F(4,3,2) \ge 1+8 = 9$. Therefore $F(4,3,2) = 9$.

Theorem 3.18 (Dual LPB for orthogonal arrays)**.** *If there exists a polynomial*

$$f(x) = 1 + f_1 K_1(x) + f_2 K_2(x) + \cdots + f_n K_n(x),$$

such that the following conditions hold:

$$\begin{aligned} f_k &\le 0, \qquad \text{for } k = t+1, \ldots, n \\ f(j) &\ge 0, \qquad \text{for } j = 0, 1, \ldots, n \end{aligned} \tag{19}$$

then the number M of any $OA(M, nq, t)$ is $M \ge f(0)$, that is,

$$F(n,q,t) \ge f(0).$$

Proof. Suppose $A_0, A_1, \ldots, A_n$ satisfy the conditions of Theorem 3.17, i.e. $A_0 \ge 1$, $A_i \ge 0$ for $i = 1, \ldots, n$, and

$$\begin{aligned} A_0 K_k(0) + \sum_{i=1}^{n} A_i K_k(i) &\ge 0 \qquad \text{for } k = 0, 1, \ldots, n \\ A_0 K_k(0) + \sum_{i=1}^{n} A_i K_k(i) &= 0 \qquad \text{for } k = 1, \ldots, t \end{aligned}$$

Multiplying the above inequalities and equalities by f_k, where $f_k \le 0$ for $k = t+1, \ldots, n$, and summarizing them for $k = 1, \ldots, n$ we obtain

$$A_0(f(0) - 1) + \sum_{i=1}^{n} A_i (f(i) - 1) \le 0, \qquad \text{thus} \qquad A_0 f(0) + \sum_{i=1}^{n} A_i f(i) \le A_0 + \sum_{i=1}^{n} A_i.$$

But according to the conditions of the theorem $A_i f(i) \ge 0$. Hence $A_0 f(0) \le A_0 + \sum_{i=1}^{n} A_i$.

Note that $A_0 > 1$ means that any vector of the array is repeated A_0 times. □

Example 3.?. Let us determine $F(4,3,3)$. Let $\mathbf{f} = (f_1, f_2, f_3, f_4)^\tau$. We have to solve the following linear programming problem: Find $\max \mathbf{B}^\tau \mathbf{f}$, where $\mathbf{B}^\tau = (8, 24, 32, 16) = (K_k(0))$ under constrains

$$\mathbf{V}\mathbf{f} \ge (-1, -1, -1, -1)^\tau, \quad f_1 + f_2 + f_3 + f_4 \ge -1, \quad f_4 \le 0.$$

$$\mathbf{V} = (K_k(j)) = \begin{pmatrix} 5 & 2 & -1 & -4 \\ 6 & -3 & -3 & 6 \\ -4 & -4 & 5 & -4 \\ -8 & 4 & -2 & 1 \end{pmatrix}.$$

The Matlab command is

```
[f,fval]=linprog(-B,-[ones(4,1) V [0 0 0 -1]']',[ones(5,1);0],[],[])
```

The result is

$$f_1 = \frac{3}{4},\ f_2 = \frac{1}{2},\ f_3 = \frac{1}{4},\ f_4 = 0, \qquad max = 26.$$

Hence $F(4,3,3) \geq 27$.

On the other hand the $[4,3,2]_3$ code is $OA(27,4,3,3)$. Therefore $F(4,3,3) = 27$.

Definition 3.19. *Let C be an $(n,M,d)_q$ code (nonlinear in general) over $\mathbb{Z}_q$ or $GF(q)$ with distance distribution $\{A_i\}_{i=0}^n$. The set of nonnegative numbers*

$$B_k = \sum_{i=0}^{n} A_i K_k(i) \qquad k = 0,1,\ldots,n,$$

is called ***MacWilliams transform*** *of $\{A_i\}_{i=0}^n$. The integer $d^\perp$ such that $B_1 = \cdots = B_{d^\perp - 1} = 0$, $B_{d^\perp} > 0$ is called* ***dual distance of C.***

Recall that the generating function of $\{B_k\}_{k=0}^n$ is

$$\frac{1}{M} W_C(x + (q-1)y, x - y),$$

where $W_C(x,y) = \sum_{i=0}^n A_i x^{n-i} y^i$ is the generating function of $\{A_i\}_{i=0}^n$.

Theorem 3.20. *If C is an $(n,M,d)_q$ code with dual distance $d^\perp$ then it is an $OA(n,M,q,t)$ with strength $t = d^\perp - 1$. Conversely, an $OA(n,M,q,t)$ is an $(n,M,d)_q$ code with dual distance $d^\perp \geq t+1$. If t is the maximal strength of the orthogonal array then $d^\perp = t+1$.*

Proof. Let $\{A_i\}_{i=0}^n$ be the distance distribution of C and $t = d^\perp - 1$. The proof of Lemma 3.12 shows that $\sum_{i=0}^n A_i K_k(i) = 0$ for $k = 1,\ldots,t$ implies

$$\left| \sum_{\mathbf{x} \in C} \chi_{\mathbf{x}}(\mathbf{z}) \right|^2 = 0 \qquad \text{thus} \qquad \sum_{\mathbf{x} \in C} \chi_{\mathbf{z}}(\mathbf{x}) = \sum_{\mathbf{x} \in C} \chi_{\mathbf{x}}(\mathbf{z}) = 0$$

for any $\mathbf{z} \in \mathbb{Z}_q^n$ of weight $1 \leq \mathrm{wt}(\mathbf{z}) \leq t$. Now Lemma 3.16 gives that C is an $OA(n,M,q,t)$.

Conversely, let C be an $OA(n,M,q,t)$. Hence C is an $(n,M)_q$ code and let $\{A_i\}_{i=0}^n$ be its distance distribution. According to Lemma 3.16

$$\sum_{\mathbf{v} \in C} \chi_{\mathbf{u}}(\mathbf{v}) = 0,$$

for any $\mathbf{u} \in \mathbb{Z}_q^n$ of weight $1 \le \mathrm{wt}(\mathbf{u}) \le t$. Now following the proof of Lemma 3.12 we get

$$\sum_{i=0}^{n} MA_i K_k(i) = \sum_{\mathbf{u}\in W_k} \left| \sum_{\mathbf{v}\in C} \chi_{\mathbf{v}}(\mathbf{u}) \right|^2 = \sum_{\mathbf{u}\in W_k} \left| \sum_{\mathbf{v}\in C} \chi_{\mathbf{u}}(\mathbf{v}) \right|^2 = 0, \qquad k = 1, \ldots, t.$$

Hence $d^{\perp} \ge t+1$. If $d^{\perp} \ge t+2$ then the first statement of the theorem gives strength at least $t+1$. This observation proves the last statement of the theorem. □

Definition 3.21. *Let C be an $(n,M)_q$ code over $\mathbb{Z}_q$ and $\mathbf{x} \in \mathbb{Z}_q^n$ be a fixed vector. The set of integers $\mathbf{p}(\mathbf{x}) = (p_0, p_1, \ldots, p_n)$ defined by*

$$p_i = |\{\mathbf{u} \in C \mid d(\mathbf{x},\mathbf{u}) = i\}|$$

*is called the **distance distribution of C with respect to** $\mathbf{x}$.*

Lemma 3.22. *Let C be $OA(M,n,q,t)$ and $\mathbf{x} \in \mathbb{F}_q^n$. If $\mathbf{p}(\mathbf{x}) = (p_0, p_1, \ldots, p_n)$ is the distance distribution of C with respect to $\mathbf{x}$ then*

$$\sum_{i=0}^{n} p_i K_k(i) = 0 \qquad \text{for } k = 1, \ldots, t. \tag{20}$$

Proof. According to Lemma 3.10

$$p_i K_k(i) = \sum_{\substack{\mathbf{u}\in C \\ d(\mathbf{x},\mathbf{u})=i}} \sum_{\mathbf{v}\in W_k} \chi_{\mathbf{u}-\mathbf{x}}(\mathbf{v}) = \sum_{\mathbf{v}\in W_k} \left(\chi_{-\mathbf{x}}(\mathbf{v}) \sum_{\substack{\mathbf{u}\in C \\ d(\mathbf{x},\mathbf{u})=i}} \chi_{\mathbf{u}}(\mathbf{v}) \right).$$

Summarizing on $i = 0, 1, \ldots, n$ we have

$$\sum_{i=0}^{n} p_i K_k(i) = \sum_{\mathbf{v}\in W_k} \left(\chi_{-\mathbf{x}}(\mathbf{v}) \sum_{i=0}^{n} \sum_{\substack{\mathbf{u}\in C \\ d(\mathbf{x},\mathbf{u})=i}} \chi_{\mathbf{u}}(\mathbf{v}) \right) = \sum_{\mathbf{v}\in W_k} \left(\chi_{-\mathbf{x}}(\mathbf{v}) \sum_{\mathbf{u}\in C} \chi_{\mathbf{u}}(\mathbf{v}) \right)$$

But according to Lemma 3.16

$$\sum_{\mathbf{u}\in C} \chi_{\mathbf{u}}(\mathbf{v}) = \sum_{\mathbf{u}\in C} \chi_{\mathbf{v}}(\mathbf{u}) = 0,$$

for $1 \le \mathrm{wt}(\mathbf{v}) \le t$. Hence $\sum_{i=0}^{n} p_i K_k(i) = 0$, for $1 \le k \le t$. □

Theorem 3.23. *Let C be $OA(M,n,q,t)$ and $\mathbf{v} \in \mathbb{F}_q^n$. If $\mathbf{p}(\mathbf{v}) = (p_0, p_1, \ldots, p_n)$ is the distance distribution of C with respect to $\mathbf{v}$ then for any polynomial $f(x)$ of degree $\deg f \le t$*

$$\sum_{i=0}^{n} p_i f(t_i) = a_0 M \qquad \text{for } k = 0, 1, \ldots, t, \tag{21}$$

where $f(x) = a_0 + \sum_{j=1}^{t} a_j Q_j(x)$

Proof. Substituting $t = t_i$ and multiplying by p_i we get

$$p_i f(t_i) = a_0 p_i + \sum_{j=1}^{t} a_j p_i Q_j(t_i), \quad \text{for } i = 0,1,\ldots,n.$$

Summarizing on i we obtain

$$\sum_{i=0}^{n} p_i f(t_i) = a_0 \sum_{i=0}^{n} p_i + \sum_{j=1}^{t} \left(a_j \sum_{i=0}^{n} p_i Q_j(t_i) \right) = a_0 M + \sum_{j=1}^{t} \left(\frac{a_j}{\binom{n}{j}(q-1)^j} \sum_{i=0}^{n} p_i K_j(i) \right)$$

Since C has strength t then according to Lemma 3.22

$$\sum_{i=0}^{n} p_i K_j(i) = 0, \quad \text{for } i = 1,\ldots,t.$$

Hence

$$\sum_{i=0}^{n} p_i f(t_i) = a_0 M.$$

□

Taking $f(x) = x^k, \quad k = 0,1,\ldots,t$ we obtain as a corollary the following theorem

Theorem 3.24. *Let C be $OA(M,n,q,t)$ and $\mathbf{v} \in \mathbb{F}_q^n$. If $\mathbf{p}(\mathbf{v}) = (p_0, p_1, \ldots, p_n)$ is the distance distribution of C with respect to $\mathbf{v}$ then*

$$\sum_{i=0}^{n} p_i t_i^k = b_k M \qquad \text{for } k = 0,1,\ldots,t, \tag{22}$$

where $t^k = b_k + \sum_{j=1}^{k} a_j Q_j(t)$ and $t_i = 1 - \frac{2i}{n}$.

Substituting $f(x) = \left(\frac{(1-x)n}{2}\right)^k, \quad k = 0,1,\ldots,t$ in Theorem 3.23 we obtain an equivalent to (22) system:

Theorem 3.25. *Let C be $OA(M,n,q,t)$ and $\mathbf{v} \in \mathbb{F}_q^n$. If $\mathbf{p}(\mathbf{v}) = (p_0, p_1, \ldots, p_n)$ is the distance distribution of C with respect to $\mathbf{v}$ then*

$$\sum_{i=0}^{n} p_i i^k = \frac{M}{q^n} \sum_{i=0}^{n} \binom{n}{i} i^k (q-1)^i \qquad \text{for } k = 0,1,\ldots,t, \tag{23}$$

Substituting $f(x) = \left(\frac{(1+x)n}{2}\right)^k, \quad k = 0,1,\ldots,t$ in Theorem 3.23 we obtain another equivalent to (22) system:

Theorem 3.26. *Let C be $OA(M,n,q,t)$ and $\mathbf{v} \in \mathbb{F}_q^n$. If $\mathbf{p}(\mathbf{v}) = (p_0, p_1, \ldots, p_n)$ is the distance distribution of C with respect to $\mathbf{v}$ then*

$$\sum_{i=0}^{n} p_i (n-i)^k = \frac{M}{q^n} \sum_{i=0}^{n} \binom{n}{i} (n-i)^k (q-1)^i \qquad \text{for } k = 0,1,\ldots,t, \tag{24}$$

Varying the polynomial $f(x)$ we obtain many equivalent linear systems for the distance distribution of the studied orthogonal array. For example

$$f(x) = (-xn)^k,\ f(x) = \left(\frac{(1-3x)n}{2}\right)^k,\ f(x) = ((1+2x)n)^k,\ f(x) = \left(\frac{(-1-3x)n}{2}\right)^k$$

corresponds to systems with matrices (m_{ki}) :

$$m_{ki} = (2i-n)^k, \quad m_{ki} = (3i-n)^k, \quad m_{ki} = (3n-4i)^k, \quad m_{ki} = (3i-2n)^k$$

Upper bounds for $\mathbf{p} = (p_0, p_1, \ldots, p_n)$**.** The above two theorems as well as similar results obtained by varying the polynomial $f(x)$ in Theorem 3.23 enable to improve upper bounds for p_i. The trivial bound is $p_i \leq M$. But dividing the right sides of (23) and (24) by the coefficients at p_i we obtained upper bounds for p_i. The linear systems (23) and (24) gives improvement only for the right and left end of $\mathbf{p}$ but combining both results (as well as with the results from other similar linear systems) we can obtain an significant improvement. For example in the case of $OA(M = 36, n = 16, q = 3, t = 2)$ we can obtain

$$\mathbf{p} \leq (1,1,1,2,2,3,5,7,12,21,32,34,24,15,10,6,4)$$

With the method described below we can find all possible distance distributions and to check that the maximums of each p_i are

$$\mathbf{p}_{max} = (1,1,1,2,2,3,4,7,12,20,32,32,24,14,8,5,4).$$

One can observe that the obtained upper bound differs from the exact value only in several positions. Hence it is almost sharp.

How to determine all possible distance distributions $\mathbf{p} = (p_0, p_1, \ldots, p_n)$**.**

The obvious number of potential solutions of (23) (and any equivalent to it linear system) is $(M+1)^{n+1}$. For the given above example of $OA(M = 36, n = 16, q = 3, t = 2)$ this number is $37^{18} \approx 10^{28} \approx 2^{94}$, which is enormous. The obtained upper bound reduce it to 6 088 642 560, but this number is still large for a direct check by replacing in the system. Hence we choose another approach.

Keeping in the mind that any solution of a linear system is a sum of a partial solution and a vector of null space of the system's matrix we prove the following

Theorem 3.27. *Let $\mathbf{V} = (j^i),\ i = 0,1,\ldots,t,\ j = 1,2,\ldots,n$. For $t < m \leq n$ the vector*

$$\left(1, -\binom{m}{1}, \binom{m}{2}, \ldots, (-1)^j \binom{m}{j}, \ldots, (-1)^m, 0, \ldots, 0\right)$$

and all $n-m-1$ its cyclic right shifts are linear independent and belong to the null-space of $\mathbf{V}$. In partial for $m = t+1$ they form a basis of the null-space.

Proof. □

Therefore any solution of (23) is a sum of a partial solution and a linear combination of the rows of the matrix form by vectors given in Theorem 3.27. Instead of this matrix we can use its "systematic" form: all without $t+1$ fixed columns have only one 1 and zeros in the others positions. Then the $n-t$ free variable can be chosen nonnegative and nongreater than the upper bound. Distance distribution is any vector with nonnegative values in the fixed $t+1$ positions. Due to the special form of the matrix generating the null space formulas for the values in the chosen $t+1$ columns can be given. We demonstrate this fact by the following example.

Example Let us consider $OA(M=18, n=7, q=3, t=2)$. The matrix $\mathbf{A}$ and the column $\mathbf{b}$ of free terms of (23) are

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 49 & 36 & 25 & 16 & 9 & 4 & 1 & 0 \end{pmatrix}; \qquad \mathbf{b} = \begin{pmatrix} 1 \\ 42 \\ 126 \end{pmatrix};$$

A partial solution of the system is $(0,0,0,0,18,-12,12,0)$. The matrix generating the null space is

$$\mathbf{A}^{\perp} = \begin{pmatrix} 1 & -3 & 3 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -3 & 3 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -3 & 3 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -3 & 3 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -3 & 3 & -1 \end{pmatrix}$$

The systematic form (reduce row echelon form (rref)) is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & -21 & 35 & -15 \\ 0 & 1 & 0 & 0 & 0 & -15 & 24 & -10 \\ 0 & 0 & 1 & 0 & 0 & -10 & 15 & -6 \\ 0 & 0 & 0 & 1 & 0 & -6 & 8 & -3 \\ 0 & 0 & 0 & 0 & 1 & -3 & 3 & -1 \end{pmatrix}$$

The partial solution can be chosen with only $t+1$ nonzero coordinates in the positions where the obtained upper bound has maximal values. In the case of $OA(36,16,3,2)$ a suitable partial solution is $(0,0,0,0,0,0,0,0,0,72,-96,60,0,0,0,0)$.