On extremal orthogonal arrays

Sho Suda (National Defense Academy of Japan)
joint work with
Alexander Gavrilyuk (Shimane University, Japan)

March 13, 2024
Number Theory and Combinatorics Seminar
University of Lethbridge

Introduction

- Orthogonal arrays were introduced by Rao in 1946 and appeared in statistics. Later, applications were found, for examples:
  - authentication codes;
  - (t, w)-threshold schemes.

Introduction

- Orthogonal arrays were introduced by Rao in 1946 and appeared in statistics. Later, applications were found, for examples:
  - authentication codes;
  - (t, w)-threshold schemes.

Definition (Orthogonal arrays)

An *orthogonal array* $\mathrm{OA}(N, n, q, t)$ is an $N \times n$ matrix M with entries the numbers $0, 1, \ldots, q-1$ such that in any $N \times t$ submatrix of M all possible row vectors of length t occur $\lambda := \frac{N}{q^t}$ times.

- Orthogonal arrays were introduced by Rao in 1946 and appeared in statistics. Later, applications were found, for examples:
  - authentication codes;
  - (t, w)-threshold schemes.

Definition (Orthogonal arrays)

An *orthogonal array* $\mathrm{OA}(N, n, q, t)$ is an $N \times n$ matrix M with entries the numbers $0, 1, \ldots, q-1$ such that in any $N \times t$ submatrix of M all possible row vectors of length t occur $\lambda := \frac{N}{q^t}$ times.

Example: $\mathrm{OA}(N = 8, n = 4, q = 2, t = 3)$, 8×4 matrix with 2 symbols

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Introduction

- Orthogonal arrays were introduced by Rao in 1946 and appeared in statistics. Later, applications were found, for examples:
  - authentication codes;
  - (t, w)-threshold schemes.

Definition (Orthogonal arrays)

An *orthogonal array* $\mathrm{OA}(N, n, q, t)$ is an $N \times n$ matrix M with entries the numbers $0, 1, \ldots, q-1$ such that in any $N \times t$ submatrix of M all possible row vectors of length t occur $\lambda := \frac{N}{q^t}$ times.

Example: $\mathrm{OA}(N = 8, n = 4, q = 2, t = 3)$, 8×4 matrix with 2 symbols

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Any 8×3 submatrix have rows $000, 001, \ldots, 111$ exactly $\lambda = \frac{8}{2^3} = 1$ time.

Research on orthogonal arrays

1. Construction: Using finite fields, (linear) codes, Hadamard matrices, etc.
2. Restriction of parameters: Rao's bound, etc.
3. Structure: Association schemes, automorphism groups, etc.
4. Applications

In this talk, I will review constructions and Rao's bound, and deal with orthogonal arrays which attain Rao's bound and are close to it in a sense.

Construction: finite fields

Theorem (Bush, 1952)

For a prime power q and a positive integer $t \geq 1$, OA$(q^t, q+1, q, t)$ exists.

Proof: Let $f_1, \dots, f_N$ be the polynomials of degree at most $t-1$ in $\mathbb{F}_q[x]$, where $N = q^t$. Define an $N \times q$ matrix M with rows indexed by $\{1, \dots, N\}$ and columns indexed by the elements of $\mathbb{F}_q$ as

$$M_{i,\alpha} = f_i(\alpha).$$

Append the column to the matrix M to make $N \times (q+1)$ matrix M' so that

$$(M')_{i,q+1} = \text{the coefficient of } x^{t-1} \text{ in } f_i.$$

Then M' is an OA$(N, q+1, q, t)$.

Construction: finite fields

Theorem (Bush, 1952)

For a prime power q and a positive integer $t \geq 1$, $\mathrm{OA}(q^t, q+1, q, t)$ exists.

Example for $q = 2$ and $t = 2$.

- $(f_1, \dots, f_4) = (0, 1, x, x+1)$: the polynomials of degree at most 1 in $\mathbb{F}_2[x]$
- Define a 4×2 matrix M by $M_{i,\alpha} = f_i(\alpha)$ and append the column to M to make M':

$$M' = \begin{array}{l c} & \begin{array}{ccc} 0 & 1 & * \end{array} \\ \begin{array}{l} f_1 = 0 \\ f_2 = 1 \\ f_3 = x \\ f_4 = x+1 \end{array} & \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \end{array}$$

  where * is the column of the coefficient of x in f_i.
- Then M' is an $\mathrm{OA}(4, 3, 2, 2)$.

Construction: finite fields

For $q = 2^m$ and $t = 3$, one more column can be added.

Theorem (Bush, 1952)

For $q = 2^m$, $\mathrm{OA}(q^3, q+2, q, 3)$ exists.

Construction: Append to the constructed matrix M' one column defined by i-th entry equal to the coefficient of x in the polynomial $f_i(x)$.
Example for $q = 2$.

- $(f_1, \ldots, f_8) = (0, 1, x, x+1, x^2, 1+x^2, x+x^2, 1+x+x^2)$: the polynomials of degree at most 2 in $\mathbb{F}_2[x]$
- Define a 8×4 matrix $M'' = (M', **)$ where M' is the same as before and $**$ is the column of the coefficient of x in f_i.
- Then M'' is an $\mathrm{OA}(8, 4, 2, 3)$.

$$\begin{array}{c c} & \begin{array}{cccc} 0 & 1 & * & ** \end{array} \\ \begin{array}{c} f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \\ f_8 \end{array} & \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \end{array}$$

Construction: Hadamard matrices

- A Hadamard matrix of order n is an $n \times n$ matrix H with entries in $\{1, -1\}$ such that $HH^\top = nI$.
- Examples: $-$ stands for -1

$$H = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}, \quad H = \begin{pmatrix} - & - & - & - \\ 1 & 1 & - & - \\ - & 1 & - & 1 \\ 1 & - & - & 1 \end{pmatrix}.$$

- The order of a Hadamard matrix is $1, 2$ or a multiple of four. The other implication is known as the Hadamard conjecture.
- The smallest order for which no Hadamard matrix is known is 668. Until 2005, it was 428. Kharaghani and Tayfeh-Razaie constructed a Hadamard matrix of order 428.
- Many constructions: the Kronecker product, Paley digraphs, the plug-in method in orthogonal designs, etc.

Construction: Hadamard matrices

- A Hadamard matrix of order n is an $n \times n$ matrix H with entries in $\{1, -1\}$ such that $HH^\top = nI$.

Theorem

1. Let H be a Hadamard matrix of order n. Then the matrix
$$M = \begin{pmatrix} H \\ -H \end{pmatrix}$$
is an OA$(2n, n, 2, 3)$.
2. Conversely, any OA$(2n, n, 2, 3)$ is obtained in this way by a Hadamard matrix of order n.

Construction: linear codes

- Let q be a prime power, and $\mathbb{F}_q$ be the finite field of order q.
- A linear code of length n over $\mathbb{F}_q$ is a subspace of the vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$.
- For $x = (x_i)_{i=1}^n, y = (y_i)_{i=1}^n \in \mathbb{F}_q^n$, define the Hamming distance between x and y by
$$d(x, y) = |\{i \in \{1, \dots, n\} \mid x_i \neq y_i\}|.$$
- For a linear code C, the minimum distance d is $\min\{d(x, y) \mid x, y \in C, x \neq y\}$.
- The dual code $C^\perp$ of C is $\{y \in \mathbb{F}_q^n \mid \langle x, y\rangle = 0$ for any $x \in C\}$, where $\langle x, y\rangle = \sum_{i=1}^n x_i y_i$.

Theorem

Let C be a linear code of length n over $\mathbb{F}_q$ such that the dual code $C^\perp$ has minimum distance $d^\perp$. Then the matrix whose rows consist of the vectors of C is an OA$(|C|, n, q, d^\perp - 1)$.

Tight orthogonal arrays

The lower bound for N on OA(N,n,q,t) was given by Rao as follows:

$$N \geq \begin{cases} \sum_{k=0}^{e} \binom{n}{k}(q-1)^k \text{ if } t=2e, \\ \sum_{k=0}^{e} \binom{n}{k}(q-1)^k + \binom{n-1}{e}(q-1)^{e+1} \text{ if } t=2e+1. \end{cases} \tag{1}$$

An OA is said to be *tight* if it achieves (1).

Tight orthogonal arrays

The lower bound for N on OA(N, n, q, t) was given by Rao as follows:

$$N \geq \begin{cases} \sum_{k=0}^{e} \binom{n}{k}(q-1)^k \text{ if } t = 2e, \\ \sum_{k=0}^{e} \binom{n}{k}(q-1)^k + \binom{n-1}{e}(q-1)^{e+1} \text{ if } t = 2e+1. \end{cases} \quad (1)$$

An OA is said to be *tight* if it achieves (1).

- Define the *degree set* of an orthogonal array M by

$$S(M) := \{d(x, y) \mid x, y \text{ are distinct rows of } M\}.$$

- $s := |S(M)|$ is said to be *degree*.
- Define $K_{n,q,j}(x) = \sum_{k=0}^{j}(-1)^k(q-1)^{j-k}\binom{x}{j}\binom{n-x}{j-k}$, known as Krautchouk polynomials.

Tight orthogonal arrays

The lower bound for N on OA(N,n,q,t) was given by Rao as follows:

$$N \geq \begin{cases} \sum_{k=0}^{e} \binom{n}{k}(q-1)^k \text{ if } t = 2e, \\ \sum_{k=0}^{e} \binom{n}{k}(q-1)^k + \binom{n-1}{e}(q-1)^{e+1} \text{ if } t = 2e+1. \end{cases} \tag{1}$$

An OA is said to be *tight* if it achieves (1).

- Define the *degree set* of an orthogonal array M by

$$S(M) := \{d(x,y) \mid x, y \text{ are distinct rows of } M\}.$$

- $s := |S(M)|$ is said to be *degree*.
- Define $K_{n,q,j}(x) = \sum_{k=0}^{j}(-1)^k(q-1)^{j-k}\binom{x}{j}\binom{n-x}{j-k}$, known as Krautchouk polynomials.

Theorem (Delsarte 1973, Noda 1986)

Let M be a tight OA(N,n,q,t). Then $s = [(t+1)/2]$, and $n \in S(M)$ if t odd, and

$$|M| \prod_{\alpha \in S(M)\setminus\{n\}} (1 - x/\alpha) = \sum_{j=0}^{[t/2]} K_{n-\varepsilon,q,j}(x),$$

where ε is 0 if t even and 1 if t odd.

Tight orthogonal arrays with even strength

Theorem (Delsarte 1973, Noda 1986)

Let M be a tight OA(N, n, q, t). Then $s = [(t+1)/2]$, and $n \in S(M)$ if t odd, and

$$|M| \prod_{\alpha \in S(M) \setminus \{n\}} (1 - x/\alpha) = \sum_{j=0}^{[t/2]} K_{n-\varepsilon,q,j}(x),$$

where ε is 0 if t even and 1 if t odd.

In particular, if there exists a tight OA$(N, n, q, 2e)$, $\sum_{j=0}^{e} K_{n,q,j}(x)$ has exactly e distinct integral zeros in the interval $[1, n]$.

Tight orthogonal arrays with even strength

Theorem (Delsarte 1973, Noda 1986)

Let M be a tight OA(N, n, q, t). Then $s = [(t+1)/2]$, and $n \in S(M)$ if t odd, and

$$|M| \prod_{\alpha \in S(M) \setminus \{n\}} (1 - x/\alpha) = \sum_{j=0}^{[t/2]} K_{n-\varepsilon,q,j}(x),$$

where ε is 0 if t even and 1 if t odd.

In particular, if there exists a tight OA$(N, n, q, 2e)$, $\sum_{j=0}^{e} K_{n,q,j}(x)$ has exactly e distinct integral zeros in the interval $[1, n]$. This yields non-existence results for

- $e = 2, q \neq 6$ by Noda (1979)
- $e \geq 3, q \geq 3$ by Hong (1986)
- $e = 3, q = 2$ and $e = 4, 5, 6, q = 2, n \leq 10^9$ by Mukerjee and Kageyama (1994)

The case $e = 2, q = 6$ was ruled out by Gavrilyuk-S.-Vidali (2019) using association schemes. Note that there are many tight OA$(N, n, q, 2)$.

Tight orthogonal arrays with even strength

The remaining cases for classification of tight OA$(N, n, q, 2e)$ are:

- q arbitrary, $e = 1$ with $n \geq 2$ (It seems that the classification is hopeless, because there are many examples and essentially this includes the classification of Hadamard matrices.)
- $q = 2$ and $e \geq 4$ with $n \geq 2e + 1$

Open Problem

Can we show the non-existence for tight OA$(N, n, 2, 2e)$ for $e \geq 4$ with $n \geq 2e$? (Existence of a non-integer root of the polynomial

$$\sum_{j=0}^{e} K_{n,2,j}(x) = \sum_{j=0}^{e} \sum_{k=0}^{j} (-1)^k \binom{x}{j} \binom{n-x}{j-k}$$

implies an affirmative answer above.)

For $e = 4$, the following are the roots of $\sum_{j=0}^{4} K_{n,2,j}(x) = 0$:

$$x = \frac{1}{2}\left(n + 1 \pm \sqrt{3n - 7 \pm \sqrt{6n^2 - 30n + 40}}\right).$$

Tight orthogonal arrays with odd strength

Theorem

Let C be a tight $\mathrm{OA}(N, n, q, 2e+1)$.
Then $C_i = \{(x_2, \ldots, x_n) \mid (i, x_2, \ldots, x_n) \in C\}$ is a tight $\mathrm{OA}(N, n-1, q, 2e)$.

- There are no tight $\mathrm{OA}(N, n, q, 2e+1)$ with $2e+1 \geq 5$ and $q \geq 3$.

Theorem (Noda, 1986)

Let C be a tight $\mathrm{OA}(N, n, q, 3)$. Then one of the following holds:

1. $(N, n, q) = (2n, n, 2)$ with $n \equiv 0 \pmod 4$,
2. $(N, n, q) = (q^3, q+2, q)$ with q even.

- The first case is equivalent to a Hadamard matrix of order n.
- The second case exists if q is a power of 2. C_i, $1 \leq i \leq q$, a complete set of MOLS of order q. The value q is conjectured to be a power of 2.

Tight OA$(q^3, q+2, q, 3)$

Theorem (Noda, 1986)

Let C be a tight OA$(N, n, q, 3)$. Then one of the following holds:

1. $(N, n, q) = (2n, n, 2)$ with $n \equiv 0 \pmod 4$,
2. $(N, n, q) = (q^3, q+2, q)$ with q even.

Theorem (Gavrilyuk-S., 2022)

If there exists a tight OA$(q^3, q+2, q, 3)$ with $q > 2$, then q is a multiple of four.

- It is known by Delsarte (1974) that a tight OA$(q^3, q+2, q, 3)$ yields a symmetric association scheme of 2 classes ($=$ a strongly regular graph).

Sketch of proof:

1. The 2-class association schemes has a 3-class fission scheme.
2. Calculating triple intersection numbers of the 3-class scheme yields the condition $q \equiv 0 \pmod 4$ if $q > 2$.

For the details of the proof and association schemes, please search my recorded talk at "Stinson66 - New Advances in Designs, Codes and Cryptography".

Extremal orthogonal arrays

Theorem (Delsarte, 1973)

Let M be an OA(N, n, q, t) with degree s. Then $t \leq 2s$ holds, with equality if and only if M is a tight OA with $t = 2s$.

We call OA(N, n, q, t) extremal if $t \geq 2s - 1$ holds.
In the block design, the same concept was introduced and studied by Ionin and Shrikhande.

- V is a finite set with v elements, called points.
- $\mathcal{B}$ is a family of k-element subsets of V, called blocks.
- $(V, \mathcal{B})$ is a t-(v, k, λ) design if any t-element subset of V is contained exactly λ blocks.
- The degree of the design $(V, \mathcal{B})$ is the number of intersection of the distinct blocks:

$$s = |\{|B \cap B'| \mid B, B' \in \mathcal{B}, B \neq B'\}|$$

Extremal t-designs

In the block design, the same concept was introduced and studied by Ionin and Shrikhande.

- V is a finite set with v elements, called points.
- $\mathcal{B}$ is a family of k-element subsets of V, called blocks.
- $(V, \mathcal{B})$ is a t-(v, k, λ) design if any t-element subset of V is contained exactly λ blocks.
- The degree or intersection numbers of the design $(V, \mathcal{B})$ is the number of intersection of the distinct blocks:

$$s = |\{|B \cap B'| \mid B, B' \in \mathcal{B}, B \neq B'\}|$$

Theorem

1. For a $2e$-(v, k, λ) design $(V, \mathcal{B})$, $|\mathcal{B}| \geq \binom{v}{e}$.
2. For a t-design $(V, \mathcal{B})$ with s intersection numbers, $t \leq 2s$ holds, with equality if and only if $t = 2s$ and the design attains the bound in 1 (called a tight design).

Ionin and Shrikhande called t-designs with s intersection numbers extremal if $t \geq 2s - 1$.

Extremal t-designs

- V is a finite set with v-elements, called points.
- $\mathcal{B}$ is a family of k-element subsets of V, called blocks.
- $(V, \mathcal{B})$ is a t-(v, k, λ)design if any t-element subset of V is contained exactly λ blocks.
- The degree s or intersection numbers of the design $(V, \mathcal{B})$ is the number of intersection of the distinct blocks:

$$s = |\{|B \cap B'| \mid B, B' \in \mathcal{B}, B \neq B'\}|$$

Ionin and Shrikhande called t-designs with s intersection numbers extremal if $t \geq 2s - 1$.

Theorem (Ionin-Shrikhande, 1993)

Let $(V, \mathcal{B})$ be a $(2s-1)$-(v, k, λ) design with s intersection numbers $x_1, \ldots, x_s$. Then

$$\frac{(s-1)(k-s)(k-s+1)}{v-2s+2} \leq \sum_{i=1}^{s} x_i - \frac{s(s-1)}{2} \leq \frac{s(k-s)(k-s+1)}{v-2s+2},$$

with equality in the lower bound iff one of the intersection numbers is zero, and with equality in the upper bound iff $t = 2s$ (that is, $(V, \mathcal{B})$ is a tight design).

Extremal orthogonal arrays

Theorem (Gavrilyuk-S., 2024)

Let M be an extremal OA$(N, n, q, 2s-1)$ with s distinct Hamming distances with

$$\{n - d(x, y) \mid x, y \text{ are dinstinct rows of } M\} = \{x_1, \ldots, x_s\}, x_1 < \cdots < x_s.$$

Then

$$\frac{(s-1)(n-s)}{q} \leq \sum_{i=1}^{s} x_i - \frac{s(s-1)}{2} \leq \frac{s(n-s)}{q},$$

with equality in the left if and only if $x_1 = 0$, and with equality in the right if and only if M is tight

Note that for a tight OA$(N, n, q, 2s)$, $n - x_1, \ldots, n - x_s$ are uniquely determined as the zeros of the polynomial $\sum_{j=0}^{s} K_{n,q,j}(x)$.

- For distinct non-negative integers $x_1, x_2, \ldots$, define $F_j^{(k)}$ $(k \geq 1, 0 \leq j \leq k\})$ as follows: $F_0^{(k)} = 1, F_k^{(k)} = x_1 \cdots x_k$ and

$$F_j^{(k)} = F_j^{(k-1)} + (x_k - k + j)F_{j-1}^{(k-1)} \quad (k \geq 2, 1 \leq j \leq k).$$

Lemma (Gavrilyuk-S., 2024)

Let M be an extremal OA$(N, n, q, 2s-1)$ with s distinct Hamming distances with

$$\{n - d(x, y) \mid x, y \text{ are distinct rows of } M\} = \{x_1, \ldots, x_s\}, x_1 < \cdots < x_s.$$

Then, for $0 \leq \ell \leq s$,

$$\sum_{j=0}^{s} (-1)^j (n-\ell)_{s-j} \lambda_{s-j} F_j^{(s)} = \delta_{\ell,0} \prod_{i=1}^{s} (n - x_i)$$

where $\lambda_j = \frac{N}{q^j}$ and $(a)_m = a(a-1)\cdots(a-m+1)$, $(a)_0 = 1$.

Sketch of proof:
Regarding a vector $(x_1, \ldots, x_n)$ of length n with entries $\{1, \ldots, q\}$ as a set $\{(1, x_1), \ldots, (n, x_n)\}$. Fixing a row y of the OA, double counting the set

$$\{(x, I) \mid x \text{ is a row of the OA }, |I| = i, I \subset x \cap y\}$$

with some calculation yields the result.

- For distinct non-negative integers $x_1, x_2, \ldots$, define $F_j^{(k)}$ $(k \geq 1, 0 \leq j \leq k\})$ as follows: $F_0^{(k)} = 1, F_k^{(k)} = x_1 \cdots x_k$ and

$$F_j^{(k)} = F_j^{(k-1)} + (x_k - k + j)F_{j-1}^{(k-1)} \quad (k \geq 2, 1 \leq j \leq k).$$

Lemma (Gavrilyuk-S., 2024)

Let M be an extremal OA$(N, n, q, 2s-1)$ with s distinct Hamming distances with

$$\{n - d(x, y) \mid x, y \text{ are distinct rows of } M\} = \{x_1, \ldots, x_s\}, x_1 < \cdots < x_s.$$

Then, for $0 \leq \ell \leq s$,

$$\sum_{j=0}^{s} (-1)^j (n-\ell)_{s-j} \lambda_{s-j} F_j^{(s)} = \delta_{\ell,0} \prod_{i=1}^{s} (n - x_i)$$

where $\lambda_j = \frac{N}{q^j}$ and $(a)_m = a(a-1)\cdots(a-m+1)$, $(a)_0 = 1$.

Solving a system of linear equations whose unknowns are $F_j^{(s)}, 1 \leq j \leq s$ yields:

$$F_j^{(s)} = \frac{(n-s+j-1)_{j-1}}{q^{j-1}} \left(\binom{s-1}{j-1} F_1^{(s)} - \frac{((s-1)\binom{s-1}{j-1} - \binom{s-1}{j})(n-s)}{q} \right).$$

Lower bound: $\frac{(s-1)(n-s)}{q} + \frac{s(s-1)}{2} \leq \sum_{i=1}^{s} x_i$

- For distinct non-negative integers $x_1, x_2, \ldots$, define $F_j^{(k)}$ $(k \geq 1, 0 \leq j \leq k\})$ as follows: $F_0^{(k)} = 1, F_k^{(k)} = x_1 \cdots x_k$ and

$$F_j^{(k)} = F_j^{(k-1)} + (x_k - k + j)F_{j-1}^{(k-1)} \quad (k \geq 2, 1 \leq j \leq k).$$

  Then:

$$F_s^{(s)} = \frac{(n-1)_{s-1}}{q^{s-1}} \left(F_1^{(s)} - \frac{(s-1)(n-s)}{q} \right).$$

- Since $F_s^{(s)} = x_1 \cdots x_s \geq 0$ and $F_1^{(s)} = \sum_{i=1}^{s} x_i - \frac{s(s-1)}{2}$, we have

$$\frac{(s-1)(n-s)}{q} + \frac{s(s-1)}{2} \leq \sum_{i=1}^{s} x_i,$$

which proves the lower bound on $\sum_{i=1}^{s} x_i$.

Upper bound: $\sum_{i=1}^s x_i \le \frac{s(n-s)}{q} + \frac{s(s-1)}{2}$

Lemma

1. (Ionin-Shrikhande, 1993) $\sum_{j=0}^s (-1)^j F_j^{(s)} \cdot (z)_{s-j} = \prod_{i=1}^s (z - x_i)$, where z is an indeterminate.
2. (Gavrilyuk-S., 2024) $N \sum_{j=0}^s (-1)^j F_j^{(s)} \frac{(n)_{s-j}}{q^{s-j}} = \prod_{i=1}^s (n - x_i)$.

Eliminating $\prod_{i=1}^s (n - x_i)$ by setting $z = n$, and using the upper bound on s-distinct Hamming distance code:

$$N \le \sum_{k=0}^s \binom{n}{k} (q-1)^k =: M,$$

we obtain:

$$\sum_{j=0}^s (-1)^j F_j^{(s)} (n)_{s-j} \le M \sum_{j=0}^s (-1)^j F_j^{(s)} \frac{(n)_{s-j}}{q^{s-j}}.$$

Substituting

$$F_j^{(s)} = \frac{(n-s+j-1)_{j-1}}{q^{j-1}} \left(\binom{s-1}{j-1} F_1^{(s)} - \frac{((s-1)\binom{s-1}{j-1} - \binom{s-1}{j})(n-s)}{q} \right)$$

into the above inequality and simplifying this, we have

$$\sum_{i=1}^s x_i \le \frac{s(n-s)}{q} + \frac{s(s-1)}{2}.$$

Summary

- Orthogonal arrays;
- Construction by finite fields, linear codes, Hadamard matrices;
- Rao's lower bound and tight orthogonal arrays;
- Extremal orthogonal arrays.

Thank you for your attention!