A Tutorial on Orthogonal Arrays: Constructions, Bounds and Links to Error-correcting Codes

Douglas R. Stinson
David R. Cheriton School of Computer Science
University of Waterloo

Talk Outline

- $\mathsf{OA}(k, n)$ and MOLS
- $\mathsf{OA}_\lambda(k, n)$, Plackett-Burman bound, constructions, affine designs
- $\mathsf{OA}_\lambda(t, k, n)$, Rao bound, Bush bounds, Bierbrauer-Friedman bound, constructions
- linear codes and orthogonal arrays, duality
- nonlinear codes and orthogonal arrays, linear programming bounds, duality
- orthogonal arrays with a non-prime-power number of symbols

Definition

Let $k \geq 2$ and $n \geq 1$ be integers. An orthogonal array $\mathsf{OA}(k, n)$ is an $n^2 \times k$ array, A, with entries from a set X of cardinality n such that, within any two columns of A, every ordered pair of symbols from X occurs in exactly one row of A.

An $\mathsf{OA}(s + 2, n)$ is equivalent to a set of s mutually orthogonal latin squares (MOLS) of order n.

Every row of the OA corresponds to a particular cell in each of the latin squares.

Example

2 MOLS of order 3

1	2	3
2	3	1
3	1	2

1	2	3
3	1	2
2	3	1

$\mathsf{OA}(4, 3)$

1	1	1	1
1	2	2	2
1	3	3	3
2	1	2	3
2	2	3	1
2	3	1	2
3	1	3	2
3	2	1	3
3	3	2	1

Example

Consider the cells in row 1, column 1:

2 MOLS of order 3

1	2	3
2	3	1
3	1	2

1	2	3
3	1	2
2	3	1

$\mathsf{OA}(4, 3)$

1	1	1	1
1	2	2	2
1	3	3	3
2	1	2	3
2	2	3	1
2	3	1	2
3	1	3	2
3	2	1	3
3	3	2	1

Example

Consider the cells in row 3, column 2:

2 MOLS of order 3

1	2	3
2	3	1
3	1	2

1	2	3
3	1	2
2	3	1

$\mathsf{OA}(4, 3)$

1	1	1	1
1	2	2	2
1	3	3	3
2	1	2	3
2	2	3	1
2	3	1	2
3	1	3	2
3	2	1	3
3	3	2	1

Some Basic Results

Theorem 1

Let $n \geq 2$. *If there is an* $\mathsf{OA}(k, n)$, *then* $k \leq n + 1$.

Theorem 2

Let $n \geq 2$. *An* $\mathsf{OA}(n + 1, n)$ *is equivalent to any of the following designs:*

1. $n - 1$ *MOLS of order* n;
2. *an affine plane of order* n;
3. *a projective plane of order* n.

First Generalization: Higher λ

Let $k \geq 2$, $n \geq 1$ and $\lambda \geq 1$ be integers. An orthogonal array $\mathsf{OA}_\lambda(k, n)$ is a $\lambda n^2 \times k$ array, A, with entries from a set X of cardinality n such that, within any two columns of A, every ordered pair of symbols from X occurs in exactly λ rows of A.

Theorem 3 [Plackett-Burman Bound (1946)]
Let $n \geq 2$. If there is an $\mathsf{OA}_\lambda(k, n)$, then

$$k \leq \frac{\lambda n^2 - 1}{n - 1}.$$

First Proof: Variance Method

Relabel the symbols so the last row of A is $1\ 1\ \cdots\ 1$. Define $N = \lambda n^2$. For $1 \leq i \leq N-1$, let a_i denote the number of "1"s in row i of A. Then

$$\sum_{i=1}^{N-1} a_i = k(\lambda n - 1)$$

$$\sum_{i=1}^{N-1} a_i(a_i - 1) = k(k-1)(\lambda - 1)$$

$$\sum_{i=1}^{N-1} {a_i}^2 = k(k(\lambda - 1) + \lambda(n-1)).$$

Define

$$\overline{a} = \frac{k(\lambda n - 1)}{N-1}.$$

First Proof: Variance Method (cont.)

Then

$$\begin{aligned} 0 &\leq \sum_{i=1}^{N-1} (a_i - \overline{a})^2 \\ &= \sum_{i=1}^{N-1} {a_i}^2 - 2\overline{a} \sum_{i=1}^{N-1} a_i + \overline{a}^2 (N-1) \\ &= k(k(\lambda-1) + \lambda(n-1)) - \frac{k^2(\lambda n - 1)^2}{\lambda n^2 - 1} \end{aligned}$$

Therefore,

$$k(\lambda n - 1)^2 \leq (\lambda n^2 - 1)(k(\lambda - 1) + \lambda(n-1)).$$

This simplifies to yield

$$k \leq \frac{\lambda n^2 - 1}{n-1}.$$

Second Proof: Applying the Johnson Bound

Again, relabel the symbols so the last row of A is $1\,1\,\cdots\,1$. Delete the last row of A, and replace every symbol $x \neq 1$ by 0. Consider the code $\mathcal{C}$ formed by the columns of the resulting array. $\mathcal{C}$ is a binary code consisting of k vectors of length $\ell = \lambda n^2 - 1$, each of which has constant hamming weight $w = \lambda n - 1$, such that the hamming distance between any two distinct codewords is equal to $2\delta = 2\lambda(n-1)$.

Apply the second Johnson bound for constant weight binary codes:

$$|\mathcal{C}| \leq \frac{\ell\delta}{w^2 - \ell w + \ell\delta}.$$

Hence,

$$k \leq \frac{(\lambda n^2 - 1)\lambda(n-1)}{(\lambda n - 1)^2 - (\lambda n^2 - 1)(\lambda n - 1) + (\lambda n^2 - 1)\lambda(n-1)} = \frac{\lambda n^2 - 1}{n-1}.$$

Third Proof: Linear Algebra Approach

Assume that A is defined on the symbols in $\mathbb{Z}_n$. Let the columns of A be denoted $C_1, \ldots, C_k$. Let C_0 be the column vector of "0"s. For $1 \leq m \leq n-1$, construct mC_j from C_j by multiplying every entry by m (modulo n).

Let $\omega = e^{2\pi i/n}$ and define $\phi : \mathbb{Z}_n \to \mathbb{C}$ by the rule $\phi(s) = \omega^s$.

Consider the set of $1 + k(n-1)$ vectors

$$\mathcal{D} = \{\phi(C_0)\} \cup \{\phi(mC_j) : 1 \leq m \leq n-1, 1 \leq j \leq k\}.$$

It can be shown that $\langle C, D \rangle = 0$ for all $C, D \in \mathcal{D}, C \neq D$, where $\langle \cdot, \cdot \rangle$ denotes the hermitian inner product of two (complex-valued) vectors.

Since $\mathcal{D}$ consists of mutually orthogonal vectors, they are linearly independent. Hence, we have a set of $1 + k(n-1)$ linearly independent vectors in $\mathcal{C}^N$, and it follows that $1 + k(n-1) \leq N (= \lambda n^2)$.

BIBDs and Resolvable BIBDs

A (v, k, λ)-BIBD (balanced incomplete block design) is a pair $(X, \mathcal{B})$, where X is a set of v elements called points and $\mathcal{B}$ is a collection of k-subsets of X (called blocks) such that every unordered pair of points occurs in exactly λ blocks. The number of blocks is denoted by b, and each point occurs in exactly r blocks, where

$$\lambda(v-1) = r(k-1) \quad \text{and} \quad bk = vr.$$

A (v, k, λ)-BIBD, say $(X, \mathcal{B})$, is resolvable if $\mathcal{B}$ can be partitioned into r parallel classes, where each parallel consists of v/k disjoint blocks.

Equality in the Plackett-Burman Bound

A resolvable (v, ℓ, λ)-BIBD is affine resolvable if any two blocks from different parallel classes intersect in μ points. Bose showed that an affine resolvable BIBD has $v = \mu n^2$, $\ell = \mu n$ and $\lambda = (\mu n - 1)/(n - 1)$ for integers μ and n. Furthermore, there are n blocks in each parallel class and the number of parallel classes is $r = (\mu n^2 - 1)/(n - 1)$. Such a design is denoted $\mathsf{AD}(n, \mu)$.

Theorem 4

An $\mathsf{AD}(n, \mu)$ *is equivalent to An* $\mathsf{OA}_\mu(k, n)$ *where* $k = (\mu n^2 - 1)/(n - 1)$.

Proof. Suppose we have an $\mathsf{AD}(n, \mu)$. For $1 \leq i \leq r$, let the blocks in the ith parallel class be named $B_{i,1}, \ldots, B_{i,n}$. For all points $x \in B_{i,j}$, define $A[x, i] = j$. Then A is the desired OA. The construction can be reversed, proving the converse. □

Example

Here is an $\mathsf{AD}(2,2)$ (i.e., an affine resolvable $(8,4,3)$-BIBD) and the resulting $\mathsf{OA}_2(2,7,2)$:

$B_{1,0} = \{0,1,2,3\}, B_{1,1} = \{4,5,6,7\}$

$B_{2,0} = \{0,1,4,5\}, B_{2,1} = \{2,3,6,7\}$

$B_{3,0} = \{0,1,6,7\}, B_{3,1} = \{2,3,4,5\}$

$B_{4,0} = \{0,2,4,6\}, B_{4,1} = \{1,3,5,7\}$

$B_{5,0} = \{0,2,5,7\}, B_{5,1} = \{1,3,4,6\}$

$B_{6,0} = \{0,3,4,7\}, B_{6,1} = \{1,2,5,6\}$

$B_{7,0} = \{0,3,5,6\}, B_{7,1} = \{1,2,4,7\}$

	1	2	3	4	5	6	7
0	0	0	1	0	0	0	0
1	0	0	0	1	1	1	1
2	0	1	0	0	0	1	1
3	0	1	1	1	1	0	0
4	1	0	1	0	1	0	1
5	1	0	0	1	0	1	0
6	1	1	0	0	1	1	0
7	1	1	1	1	0	0	1

Existence of Affine Designs

There are only two families of $\mathsf{AD}(n, \mu)$ known to exist:

1. $\mathsf{AD}(q, q^d)$, where q is a prime power (this design consists of the hyperplanes in an affine geometry of dimension $d + 2$) and
2. $\mathsf{AD}(2, s)$, whenever a Hadamard matrix of order $4s$ exists.

The first family yields $\mathsf{OA}_{q^d}\left(\frac{q^{d+2}-1}{q-1}, q\right)$ and the second family yields $\mathsf{OA}_s(4s-1, 2)$.

An $\mathsf{OA}_s(4s-1, 2)$ is constructed from a Hadamard matrix of order $4s$ by standardizing a column of the matrix, and then deleting it.

Example

Here is a Hadamard matrix of order 8 and the resulting $\mathsf{OA}_2(2, 7, 2)$:

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & - & 1 & - & 1 & - & 1 & - \\
1 & 1 & - & - & 1 & 1 & - & - \\
1 & - & - & 1 & 1 & - & - & 1 \\
1 & 1 & 1 & 1 & - & - & - & - \\
1 & - & 1 & - & - & 1 & - & 1 \\
1 & 1 & - & - & - & - & 1 & 1 \\
1 & - & - & 1 & - & 1 & 1 & -
\end{pmatrix}$$

1	1	1	1	1	1	1
0	1	0	1	0	1	0
1	0	0	1	1	0	0
0	0	1	1	0	0	1
1	1	1	0	0	0	0
0	1	0	0	1	0	1
1	0	0	0	0	1	1
0	0	1	0	1	1	0

Second Generalization: Higher t

Let $k \geq t \geq 2$, $n \geq 1$ and $\lambda \geq 1$ be integers. An orthogonal array $\mathsf{OA}_\lambda(t,k,n)$ is a $\lambda\, n^t \times k$ array, A, with entries from a set X of cardinality n such that, within any t columns of A, every ordered t-tuple of symbols from X occurs in exactly λ rows of A.

Theorem 5 [Rao Bound (1947)]

Let $n \geq 2$. If there is an $\mathsf{OA}_\lambda(t,k,n)$, then

$$\lambda n^t \geq \begin{cases} 1 + \sum_{i=1}^{t/2} \binom{k}{i}(n-1)^i & \text{if } t \text{ is even} \\ 1 + \sum_{i=1}^{(t-1)/2} \binom{k}{i}(n-1)^i + \binom{k-1}{(t-1)/2}(n-1)^{(t+1)/2} & \text{if } t \text{ is odd.} \end{cases}$$

The Plackett-Burman bound is the special case of the Rao bound with $t = 2$.

The Case $\lambda = 1$: The Bush Bound

Theorem 6 [Bush Bound (1952)]

Let $n, t \geq 2$. If there is an $\mathsf{OA}_1(t, k, n)$, then

$$k \leq \begin{cases} n + t - 1 & \text{if } n \text{ is even and } t \leq n \\ n + t - 2 & \text{if } n \text{ is odd and } 3 \leq t \leq n \\ t + 1 & \text{if } t \geq n. \end{cases}$$

Theorem 7

If there exists an $\mathsf{OA}_\lambda(t, k, n)$, then there exists an $\mathsf{OA}_\lambda(t-1, k-1, n)$.

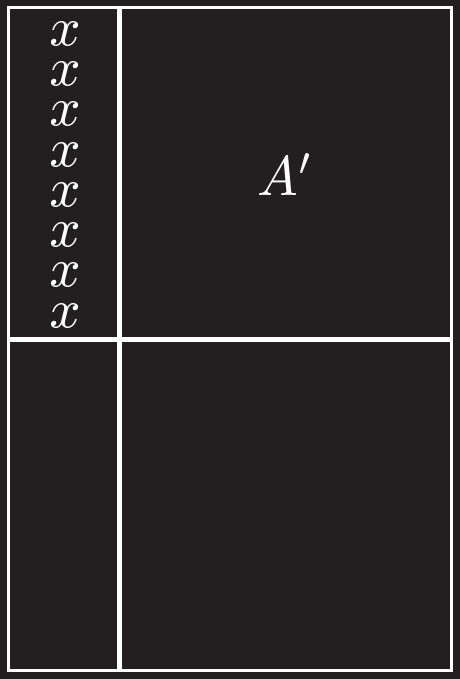
Applying Theorem 7, we have that

$$\mathsf{OA}_1(t, k, n) \Rightarrow \mathsf{OA}_1(t-1, k-1, n) \Rightarrow \cdots \Rightarrow \mathsf{OA}_1(2, k-t+2, n),$$

so $k - t + 2 \leq n + 1$ always holds. This yields the bound $k \leq n + t - 1$.

Derived OAs

Proof of Theorem 7. Let A be an $\mathsf{OA}_\lambda(t, k, n)$ and let x be any symbol. The indicated subarray A' is an $\mathsf{OA}_\lambda(t-1, k-1, n)$.



A' is formed from A by deleting all rows of A that do not contain x in the first column, and then deleting the first column. □

Example

Theorem 8

For all t and all n, there exists an $\mathsf{OA}_1(t, t+1, n)$.

Proof. For all t-tuples $(x_1, \ldots, x_t) \in (\mathbb{Z}_n)^t$, define a row of A consisting of the $(t+1)$-tuple

$$x_1 \quad x_2 \quad \cdots \quad x_t \quad -(x_1 + \cdots x_t) \bmod n.$$

That is, we write down all the $(t+1)$-tuples that sum to 0 modulo n. □

Observe that an $\mathsf{OA}_1(t, t+1, n)$ meets the Bush bound with equality if $t \geq n$.

The Case of Large t: The Bierbrauer-Friedman Bound

Theorem 9 [Bierbrauer-Friedman Bound (1995)]
Let $n, t \geq 2$. If there is an $\mathsf{OA}_\lambda(t, k, n)$, then

$$\lambda n^t \geq n^k \left(1 - \frac{(n-1)k}{n(t+1)}\right).$$

The bound is nontrivial if

$$t > \frac{(n-1)k}{n} - 1.$$

If $\lambda = 1$ and $k = t + 2$, then the bound yields $t \leq n - 1$. Hence, if $t \geq n$, it must be the case that $k \leq t + 1$. This is the third case of the Bush bound.

Simple and Linear Orthogonal Arrays

An orthogonal array A is a simple if all its rows in D are different. An orthogonal array A is linear if the symbol set $X = \mathbb{F}_q$ for some prime power q and the rows of A form a subspace (of the vector space $(\mathbb{F}_q)^k$) having dimension $\log_q |D|$.

A linear orthogonal array is necessarily simple, and λ is a power of q in a linear orthogonal array.

Constructing Linear Orthogonal Arrays

Theorem 10 [Bose (1947)]

Let q be a prime power. Suppose M is an ℓ by k matrix of elements from $\mathbb{F}_q$ such that every set of t columns of M is linearly independent, and M has rank ℓ. Define A to be the q^ℓ by k matrix whose rows consist of all the linear combinations of the rows of M. Then A is a linear $\mathsf{OA}_\lambda(t, k, q)$ where $\lambda = q^{\ell - t}$.

Example

Suppose q is a prime power, and let $\alpha \in \mathbb{F}_q$ be a primitive element. Let M be the following 2 by $q+1$ matrix:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \end{pmatrix}$$

Every pair of columns of M is linearly independent, so M generates a linear $\mathsf{OA}_1(2, q+1, q)$.

This orthogonal array is optimal; it is equivalent to a projective or affine plane of order q.

Example

We can generalize the previous example to any t such that $2 \leq t \leq q+1$. Suppose q is a prime power, and let $\alpha \in \mathbb{F}_q$ be a primitive element. Let M be the following t by $q+1$ matrix:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\ 0 & 0 & 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(q-2)} \\ 0 & 0 & 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(q-2)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 1 & \alpha^{t-1} & \alpha^{(t-1)2} & \cdots & \alpha^{(t-1)(q-2)} \end{pmatrix}$$

Every set of t columns of M is linearly independent, so M generates a linear $\mathsf{OA}_1(t, q+1, q)$. For $t = 3$ and q odd, this orthogonal array is optimal as it meets the Bush bound with equality.

Gilbert-Varshamov Bound

Theorem 11 [Gilbert (1952), Varshamov (1957)]
Let ℓ, t and k be positive integers such that $2 \leq t \leq \ell$, and let q be a prime power. Suppose that

$$\sum_{i=0}^{t-1} \binom{k-1}{i} (q-1)^i < q^\ell. \tag{1}$$

Then there exists a linear $\mathsf{OA}_\lambda(t, k, q)$, where $\lambda = q^{\ell-t}$.

Theorem 11 is proven by showing that there is an ℓ by k matrix satisfying the conditions of Theorem 10. This can be done by an easy counting argument.

Codes

Let Q be a set of q symbols. A code is a set $\mathcal{C}$ of k-tuples (of symbols) called codewords.

For $\mathbf{x}, \mathbf{y} \in Q^k$, define the Hamming distance between $\mathbf{x}$ and $\mathbf{y}$ to be

$$\mathsf{dist}(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i\}|,$$

where $\mathbf{x} = (x_1, \ldots, x_k)$ and $\mathbf{y} = (y_1, \ldots, y_k)$.

The distance of the code $\mathcal{C}$, denoted $\mathsf{dist}(\mathcal{C})$, is the smallest positive integer d such that $\mathsf{dist}(\mathbf{x}, \mathbf{y}) \geq d$ for all $\mathbf{x}, \mathbf{y} \in \mathcal{C}$, $\mathbf{x} \neq \mathbf{y}$.

$\mathcal{C}$ is a (k, M, d, q)-code if $|\mathcal{C}| = M$ and $\mathsf{dist}(\mathcal{C}) \geq d$.

Linear Codes

A code $\mathcal{C}$ is a linear code of dimension m if $Q = \mathbb{F}_q$ for some prime power q and $\mathcal{C}$ is an m-dimensional subspace of the vector space $(\mathbb{F}_q)^k$. The dual code of a linear code $\mathcal{C}$ is the code $\mathcal{C}^\perp$, where

$$\mathcal{C}^\perp = \{\mathbf{y} \in (\mathbb{F}_q)^k : \mathbf{x} \cdot \mathbf{y} = 0 \text{ for all } \mathbf{x} \in \mathcal{C}\}.$$

(As usual, "$\mathbf{x} \cdot \mathbf{y}$" denotes the inner product over $\mathbb{F}_q$ of the two vectors $\mathbf{x}$ and $\mathbf{y}$.) The subspaces $\mathcal{C}$ and $\mathcal{C}^\perp$ are called orthogonal complements of each other. Observe that $\mathcal{C}^\perp$ is a linear code of dimension $k - \dim(\mathcal{C})$.

Linear Codes and OAs

Theorem 12

Suppose that $\mathcal{C} \subseteq (\mathbb{F}_q)^k$ *is a linear code of dimension* m*. Then* $\mathsf{dist}(\mathcal{C}) \geq d$ *if and only if* $\mathcal{C}^\perp$ *is a linear* $\mathsf{OA}_\lambda(d-1, k, q)$*, where* $\lambda = q^{k-m-d+1}$.

Theorem 12 says that the theory of linear codes is "equivalent" to the theory of linear orthogonal arrays. In particular, every bound or construction for linear codes implies a corresponding bound or construction for linear orthogonal arrays, and vice versa.

Hamming and Simplex Codes

Let q be a prime power and let $r \geq 2$. The Hamming code is a linear (k, M, d, q)-code where $k = (q^r - 1)/(q - 1)$, $M = q^{k-r}$ and $d = 3$. The Simplex code is the dual of the Hamming code; it is a (k, M, d, q)-code where $k = (q^r - 1)/(q - 1)$, $M = q^r$ and $d = q^{r-1}$.

It follows that the Hamming code is an $\mathsf{OA}_\lambda(t, k, q)$ where $t = q^{r-1} - 1$, $k = (q^r - 1)/(q - 1)$ and $\lambda = q^{k-r-t}$. This is an optimal OA because it meets the Bierbrauer-Friedman bound with equality.

The Simplex code is an $\mathsf{OA}_\lambda(2, k, q)$ where $k = (q^r - 1)/(q - 1)$ and $\lambda = q^{r-2}$. This is an optimal OA because it meets the Plackett-Burman bound with equality.

Hamming and Simplex Codes (cont.)

The Simplex code can be constructed using Theorem 10. From every 1-dimensional subspace of $(\mathbb{F}_q)^r$, choose a (non-zero) vector $\mathbf{v}$. Let M be the r by $(q^r - 1)/(q - 1)$ matrix whose columns are the chosen vectors. Clearly no two columns of M are linearly dependent, so M yields an OA with $t = 2$. (Equivalently, the Hamming code has distance $d = 3$.)

When $q = 2$, the columns of M comprise all $2^r - 1$ non-zero vectors in $(\mathbb{F}_2)^r$. For example, when $r = 3$, we have

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

Rao and Sphere-packing Bounds

Recall the Rao bound for $\mathsf{OA}_\lambda(t,k,q)$ in the case of even t:

$$\lambda q^t \geq 1 + \sum_{i=1}^{t/2} \binom{k}{i} (q-1)^i.$$

Suppose $\mathcal{C}$ is a linear (k, q^m, d, q)-code where d is odd. Then $\mathcal{C}^\perp$ is a $\mathsf{OA}_\lambda(d-1,k,q)$, where $\lambda = q^{k-m-d+1}$. Applying the Rao bound with $t = d-1$, we obtain

$$q^{k-m-d+1} q^{d-1} \geq 1 + \sum_{i=1}^{(d-1)/2} \binom{k}{i} (q-1)^i,$$

or

$$q^m \leq \frac{q^k}{1 + \sum_{i=1}^{(d-1)/2} \binom{k}{i} (q-1)^i}.$$

This is the Sphere-packing bound for (linear) codes.

Bierbrauer-Friedman and Plotkin Bounds

Recall the Bierbrauer-Friedman bound for $\mathsf{OA}_\lambda(t,k,q)$:

$$\lambda q^t \geq q^k \left(1 - \frac{(q-1)k}{q(t+1)}\right).$$

Suppose $\mathcal{C}$ is a linear (k, q^m, d, q)-code. Then $\mathcal{C}^\perp$ is a $\mathsf{OA}_\lambda(d-1,k,q)$, where $\lambda = q^{k-m-d+1}$. Applying the Bierbrauer-Friedman bound with $t = d-1$, we obtain

$$q^{k-m-d+1} q^{d-1} \geq q^k \left(1 - \frac{(q-1)k}{qd}\right).$$

Suppose that $d > (q-1)k/q$; then

$$q^m \leq \frac{qd}{qd - (q-1)k}.$$

This is the Plotkin bound for (linear) codes.

A Family of Nonlinear OAs

Theorem 13 [Mudhopadhyay (1981), Bierbrauer (1995)]
Suppose q is a prime power, $\ell \geq m$ and $2 \leq t \leq q^\ell$. Then there exists an $\mathsf{OA}_{q^{(t-1)(\ell-m)}}(t, q^\ell, q^m)$.

Proof. Let $\phi : \mathbb{F}_{q^\ell} \to (\mathbb{F}_q)^m$ be any surjective $\mathbb{F}_q$-linear mapping. The rows of A are indexed by t-tuples $(z, a_1, \ldots, a_{t-1})$, where $z \in (\mathbb{F}_q)^m$ and $a_i \in \mathbb{F}_{q^\ell}$ $(1 \leq i \leq t-1)$, and the columns of A are indexed by the elements of $\mathbb{F}_{q^\ell}$. An entry $A[r, c]$ is defined as follows:

$$A[r, c] = \phi\left(\sum_{j=1}^{t-1} a_j c^j\right) + z,$$

where $r = (z, a_1, \ldots, a_{t-1})$. □

A Family of Nonlinear OAs (cont.)

For $t = 2$, we obtain $\mathsf{OA}_{q^{\ell-m}}(2, q^\ell, q^m)$. If $\ell \leq 2m$, then these OAs have the minimum possible value of λ permitted by the Plackett-Burman bound:

$$\begin{aligned} \lambda &\geq \frac{q^\ell(q^m - 1) + 1}{q^{2m}} \\ &= q^{\ell-m} - \frac{q^\ell - 1}{q^{2m}} \\ &> q^{\ell-m} - 1. \end{aligned}$$

Since λ is an integer, it must be the case that $\lambda \geq q^{\ell-m}$.

Distance Distributions of Codes

Suppose $\mathcal{C}$ is an $(k, M, d, 2)$ (binary) code. The distance distribution of $\mathcal{C}$ is defined to be the sequence $(A_0, A_1, \ldots, A_k)$, where

$$A_i = \frac{1}{M}|\{(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathsf{dist}(\mathbf{x}, \mathbf{y}) = i\}|,$$

$i = 0, \ldots, k$. The following properties are easily verified:

$$A_0 = 1, \tag{2}$$

$$A_i \geq 0 \quad \text{for } 0 \leq i \leq k, \quad \text{and} \tag{3}$$

$$A_0 + A_1 + \ldots + A_k = M. \tag{4}$$

Also,

$$A_i = 0 \text{ for } 1 \leq i \leq d-1, \text{ and } A_d > 0.$$

Krawtchouk Polynomials

Let ℓ be a non-negative integer, and let $P_\ell(x)$ be the Krawtchouk polynomial defined as follows:

$$P_\ell(x) = \sum_{j=0}^{\ell} (-1)^j \binom{x}{j} \binom{k-x}{\ell-j}.$$

The dual distance distribution of $\mathcal{C}$ is defined to be $(A_0', A_1', \ldots, A_k')$, where

$$A_i' = \frac{1}{M} \sum_{j=0}^{k} A_j P_i(j),$$

$i = 0, \ldots, k$. We will express this notationally as

$$(A_0', A_1', \ldots, A_k') = \mathsf{Kr}(A_0, A_1, \ldots, A_k).$$

Krawtchouk Polynomials (cont.)

The following properties, analogous to (2), (3) and (4), were proved by Delsarte:

$$A_0^{'} = 1, \tag{5}$$

$$A_i^{'} \geq 0 \quad \text{for } 0 \leq i \leq k, \quad \text{and} \tag{6}$$

$$A_0^{'} + A_1^{'} + \ldots + A_k^{'} = \frac{2^k}{M}. \tag{7}$$

Delsarte further showed that Kr is an involutory transformation:

$$\mathsf{Kr}(A_0^{'}, A_1^{'}, \ldots, A_k^{'}) = (A_0, A_1, \ldots, A_k). \tag{8}$$

Dual Distance

If $A_i^{'} = 0$ for $1 \leq i \leq d^{'} - 1$ and $A_{d'}^{'} > 0$, then $d^{'}$ is called the dual distance of the code $\mathcal{C}$. Suppose we write the codewords in $\mathcal{C}$ as rows of an $M \times k$ array. Delsarte proved the following important result.

Theorem 14 [Delsarte (1973)]
$\mathcal{C}$ is an $\mathsf{OA}_{M/2^{d'-1}}(d' - 1, k, 2)$.

If $\mathcal{C}$ is linear, then the dual distance distribution of $\mathcal{C}$ is the same as the distance distibution of $\mathcal{C}^{\perp}$. Hence, Theorem 14 generalizes Theorem 12.

Linear Programming Bounds

Let D and k be positive integers such that $D \leq k$. We employ the following linear program, $\mathsf{L}(k, D)$, which is due to McEliece, Rodemich, Rumsey and Welch.

Maximize $S = x_0 + x_1 + \cdots + x_k$ subject to

$$x_0 = 1$$

$$x_i = 0 \qquad \text{for } 1 \leq i \leq D-1$$

$$x_i \geq 0 \qquad \text{for } D \leq i \leq k$$

$$\sum_{j=0}^{k} x_j P_i(j) \geq 0 \qquad \text{for } 0 \leq i \leq k.$$

Linear Programming Bounds (cont.)

Theorem 15

Suppose that $\mathcal{C}$ is a $(k, M, d, 2)$ code. Then the following hold:

1. *Let S_{opt} be the optimal solution to $\mathsf{L}(k, d)$. If $\mathcal{C}$ has distance d, then $M \leq S_{\mathsf{opt}}$.*
2. *Let S_{opt} be the optimal solution to $\mathsf{L}(k, d')$. If $\mathcal{C}$ has dual distance d', then $M \geq 2^k / S_{\mathsf{opt}}$.*

Linear Programming Bounds (cont.)

Proof. Let $(A_0, A_1, \ldots, A_k)$ be the distance distribution of a $(k, M, d, 2)$ code, $\mathcal{C}$, having distance d, and let $(A_0^{'}, A_1^{'}, \ldots, A_k^{'})$ be the dual distance distribution of $\mathcal{C}$.

The first assertion is proved as follows. We claim that $(A_0, \ldots, A_k)$ is a feasible solution for $\mathsf{L}(k, d)$. The constraints of $\mathsf{L}(k, d)$ are satisfied because of (2), (3) and (6), and the fact that $\mathcal{C}$ is assumed to have distance d. Then, from (4), the resulting value of the objective function is M, so the first assertion follows.

To prove the second assertion, we show that $(A_0^{'}, \ldots, A_k^{'})$ is a feasible solution for $\mathsf{L}(k, d^{'})$. This follows in a similar way from (3), (5), (6) and (8). Then, from (7), the resulting value of the objective function is $2^k/M$, so the second assertion follows, as well. □

Duality of Bounds for Codes and OAs

Gopalakrishnan (1994) (see also Bierbrauer, Gopalakrishnan and Stinson (1998)) observed that Theorem 15 provides an elementary and transparent explanation of the "duality" of the Sphere-Packing and Rao bounds; and of the Plotkin and Bierbrauer bounds. This follows immediately from Theorem 15 once it is proven that the bounds in question are consequences of the more general linear programming bound. For example, it is known that the Sphere-Packing bound is a consequence of the Linear Programming bound. Therefore the Rao bound holds.

Some comments:

1. Other examples of "dual pairs" of bounds also exist.
2. The theory can be generalized to non-binary codes and OAs.
3. A similar observation was made by Levenshtein (1995) using a much more complicated approach.

OAs where the Number of Symbols is not a Prime Power

There is an extensive theory of MOLS, which yields many constructions for OAs with $t = 2$ on an arbitrary number of symbols.

As well, recall from Theorem 8 that an $\mathsf{OA}_1(t, t+1, n)$ exists for all t and n.

In contrast, there are very few constructions for OAs with $3 \leq t \leq k-2$, in which the number of symbols is not a prime power. One classical construction is a "direct" product construction.

Theorem 16 [Bush (1952)]
If there exist $\mathsf{OA}_{\lambda_1}(t, k, n_1)$ *and* $\mathsf{OA}_{\lambda_2}(t, k, n_2)$*, then there exists an* $\mathsf{OA}_{\lambda_1\lambda_2}(t, k, n_1 n_2)$.

OAs where the Number of Symbols is not a Prime Power (cont.)

A recent method of Kreher has been used to produce new infinite classes of $\mathsf{OA}_\lambda(3, k, n)$ with $k \geq 5$. This technique employs resolvable 3-wise balanced designs and ordered designs of strength 3. Here are two examples of results obtained using applications of this method.

Theorem 17 [Colbourn, Kreher, McSorley, Stinson (2002)]
Suppose q is an odd prime power. Then there exists an $\mathsf{OA}_{q-1}(3, q+3, q+1)$.

Theorem 18 [Colbourn, Kreher, McSorley, Stinson (2002)]
Suppose q is an odd prime power. Then there exists an $\mathsf{OA}_{q^2-1}(3, 2(q+3), q+1)$.

Applications of Orthogonal Arrays in Computer Science

- Secrecy and authentication codes
- Threshold schemes
- Perfect local randomizers
- Derandomization
- Resilient and correlation-immune functions
- Block cipher and stream cipher design

References

For more information on orthogonal arrays, including applications, see:

- J. Bierbrauer, Introduction to Coding Theory, CRC Press, 2005, Chapter 15.
- C. J. Colbourn and J. H. Dinitz. The CRC Handbook of Combinatorial Designs, CRC Press, 1996, Sections II.4 and II.5.
- A. S. Hedayat, N. J. A. Sloane and J. Stufken, Orthogonal Arrays: Theory and Applications, Springer, 1999.
- D. R. Stinson, Combinatorial Designs: Constructions and Analysis, Springer, 2004, Chapters 10 and 11.