Bounds on orthogonal arrays and resilient functions

Jürgen Bierbrauer
Mathematisches Institut der Universität
Im Neuenheimer Feld 288
69120 Heidelberg
Germany

September 6, 2001

Abstract

The only known general bounds on the parameters of **orthogonal arrays** are those given by Rao in 1947 [7] for general $OA_\lambda(t,k,v)$ and by Bush [3] in 1952 for the special case $\lambda = 1$. We present an algebraic method based on characters of homocyclic groups which yields the Rao bounds, the Bush bound in case $t \geq v$ and more importantly a new explicit bound which for large values of t (the **strength** of the array) is much better than the Rao bound. In the case of binary orthogonal arrays where all rows are distinct this bound was previously proved by Friedman [6] in a different setting. We also note an application to resilient functions.

1 The method

An *orthogonal array* with parameters $OA_\lambda(t,k,v)$ is defined as a multiset $\mathcal{A}$ of mappings from a k-set C into a v-set E such that for every choice of t distinct elements $x_1, x_2, \ldots x_t$ in C and t not necessarily distinct elements $y_1, y_2, \ldots y_t$ in E there are exactly λ elements $f \in \mathcal{A}$ affording the operation

$f(x_i) = y_i, i = 1,2,\ldots t$. We may describe $\mathcal{A}$ as a uniformly t-transitive multiset of mappings from a k-set into a v-set. $\mathcal{A}$ may be visualized as an array with set C of columns and set E of entries, where each mapping $f \in \mathcal{A}$ contributes a row.
So let $\mathcal{A}$ be an $OA_\lambda(t,k,v)$. We may impose the structure of a cyclic group on the set of entries: $E = \mathbb{Z}/v$. Likewise the set of k-tuples of entries may be given the structure of a homocyclic group. So put $G = (\mathbb{Z}/v)^k$. Then $\mathcal{A}$ is a multisubset of G. Equivalently we may consider the characteristic function $\chi_{\mathcal{A}}$ of $\mathcal{A}$. This is a function with non-negative integer values. Here $\chi_{\mathcal{A}}(x)$ is the multiplicity with which $x \in G$ occurs in $\mathcal{A}$. Consider the space $L^2(G)$ of complex-valued functions on G, with scalar product $<,>$, where

$$< f,g >= \frac{1}{\mid G \mid} \sum_{x \in G} f(x) \cdot \overline{g(x)}.$$

Here $x = (x_1, x_2, \ldots, x_k) \in G$. As is generally known the characters of G form an orthonormal basis of $L^2(G)$. This is in fact easily checked. Every element $z = (z_1, z_2, \ldots, z_k)$ yields a character ϕ_z, where

$$\phi_z(x) = \zeta^{\sum x_i \cdot z_i}.$$

Here ζ is a primitive complex $v-$th root of unity, which will be fixed throughout the discussion. We will take the liberty to write $\sum_{x \in \mathcal{A}}$ even in the presence of multiplicities > 1 in the sense that each summand x occurs $\chi_{\mathcal{A}}(x)$ times. We impose the structure of a graph on G by defining that $x, y \in G$ are neighbours ($x \perp y$) whenever their Hamming distance $d(x,y)$ equals 1. So there are two reasons for the use of the symbol G : G is a group and also a graph. Let A be the adjacency operator given by the graph G. This means that

$$(Af)(x) = \sum_{y \perp x} f(y).$$

We see that the characters of G are eigenvectors of A : In fact, denote by $wt(z)$ the Hamming weight of z. Then
$(A\phi_z)(x) = \sum_{y \perp x} \zeta^{\sum y_i \cdot z_i} = (k - wt(z))(v-1) \cdot \phi_z(x) + wt(z)\phi_z(x) \cdot \sum_{\delta \neq 0} \zeta^{\delta \cdot \rho}$.
Here $\rho \neq 0$. As the sum over all powers of ζ vanishes, the last summand in the above expression equals -1. It follows that the characters ϕ_z form an orthonormal basis of Eigenvectors of A, the Eigenvalues being

$$(k - wt(z))(v-1) - wt(z) = (v-1)k - v \cdot wt(z).$$

Express $\chi = \chi_{\mathcal{A}}$ in terms of the basis given by the characters:

$$\chi = \chi_{\mathcal{A}} = \sum_{z \in G} \mu_z \cdot \phi_z.$$

We have
$\mu_z =< \chi, \phi_z >= \frac{1}{|G|} \sum_{x \in \mathcal{A}} \zeta^{-\sum x_i \cdot z_i}$. Let now $wt(z) = t$. By definition of an orthogonal array, the projection of $\mathcal{A}$ onto the support of z consists of all the $t-$tuples (with v entries), each $t-$tuple occuring λ times. Thus $\mu_z = \frac{\lambda}{|G|} \sum_y \zeta^{-\sum y_i \cdot z_i}$. Here y runs through all $t-$tuples, and z is a given $t-$tuple, all of whose entries are nonzero. As the sum over all powers of ζ vanishes, it follows that μ_z vanishes. As $\mathcal{A}$ is an OA of any strength between 1 and t we get the following:

- $\mu_z = 0$ for every $z \in G, 0 < wt(z) \leq t.$

We are interested in lower bounds on $b = b(\mathcal{A})$, where $b = \lambda \cdot v^t = \sum_{x \in G} \chi(x)$ is the number of rows of the array. The length of χ and the coefficient μ_0 both involve the number $b:$

$$\sum_z \mid \mu_z \mid^2 =< \chi, \chi >= \frac{1}{\mid G \mid} \sum_{x \in G} \chi(x)^2 \geq \frac{1}{\mid G \mid} \cdot b,$$

$$\mu_0 =< \chi, \phi_0 >= \frac{1}{\mid G \mid} \cdot b.$$

Moreover we have by definition

$$< A\chi, \chi >= \frac{1}{\mid G \mid} \sum_{x \in G} \sum_{y \in G, y \perp x} \chi(x)\chi(y) \geq 0.$$

If we use the basis consisting of characters of G, the same expression becomes

$$< A\chi, \chi >= \sum_{z \in G} [(v-1)k - v \cdot wt(z)] \mid \mu_z \mid^2 .$$

We know μ_0 and we also know that the remaining coefficients are nonzero only if $wt(z) \geq t+1$. Assume $t > (v-1)k/v - 1$. Then the Eigenvalues in question are negative and we get

$$< A\chi, \chi > \leq k(v-1)b^2 / \mid G \mid^2 + [(v-1)k - v(t+1)]\{\frac{b}{\mid G \mid} - \frac{b^2}{\mid G \mid^2}\}.$$

The last factor of the above expression is a lower bound on $\sum_{z\neq 0} \mid \mu_z \mid^2$. We use that $< A\chi, \chi >\geq 0$. By factoring out and reordering terms this yields a lower bound on b. This bound becomes trivial if $t \leq (v-1)k/v - 1$.

Theorem 1 *If there exists an $OA_\lambda(t,k,v)$, then the following lower bound on the number $b = \lambda \cdot v^t$ holds:*

$$b \geq v^k(1 - \frac{(v-1)k}{v(t+1)}).$$

This bound is nontrivial if and only if $t > (v-1)k/v - 1$.

Consider the special case $\lambda = 1$ and assume $k = t+2$. Our bound says

$$v^t \geq v^{t+2}(1 - \frac{(v-1)(t+2)}{v(t+1)}).$$

By removing common factors and reordering terms we get $t < v$:

Corollary 1 *If an $OA_1(t,k,v)$ exists, where $t \geq v$, then*

$$k \leq t+1.$$

This is the most important case of the Bush bounds [3].

We get bounds in a different way: The array $\mathcal{A}$ can be seen as a submultiset of G, of cardinality b. More precisely we view $\mathcal{A}$ as a set of cardinality b, where each $x \in G$ contributes $\chi(x)$ elements. Consider the space $L^2(\mathcal{A})$ in analogy to the above, with the scalar product $(,)$, where

$$(f,g) = \frac{1}{b}\sum_{x\in\mathcal{A}} f(x)\cdot\overline{g(x)}.$$

Every function in $L^2(G)$ yields by restriction a function in $L^2(\mathcal{A})$. Let us check how the characters of G behave under this operation. Denote by f_z the restriction of ϕ_z to $\mathcal{A}$:

$$(f_z, f_w) = \frac{1}{b}\sum_{x\in\mathcal{A}} \phi_z(x)\cdot\overline{\phi_w(x)} = \frac{\mid G\mid}{b} < \phi_{z-w}, \chi >= \frac{\mid G\mid}{b}\mu_{z-w}.$$

We know that μ_{z-w} vanishes if $0 < wt(z-w) \leq t$. Assume now t is even. Let Z_0 consist of all elements of G of Hamming weight $\leq t/2$. If t is odd, let Z_0 consist of all tuples in G with Hamming weight $< t/2$ and of all z of weight $(t+1)/2$ having a nonzero entry in the first coordinate. In both cases the $f_z, z \in Z_0$ form a system of pairwise orthogonal vectors in $L^2(\mathcal{A})$. They are thus linearly independent. As $L^2(\mathcal{A})$ has dimension $\mid \mathcal{A} \mid= b$, we get $b \geq\mid Z_0 \mid$:

Theorem 2 (Rao) *Assume an $OA_\lambda(t,k,v)$ exists. Then the number b of rows of the array is bounded as follows:*

- *If t is even, then*
$$b \geq \sum_{i=0}^{t/2} \binom{k}{i} (v-1)^i.$$
- *If t is odd, then*
$$b \geq \sum_{i=0}^{(t-1)/2} \binom{k}{i} (v-1)^i + \binom{k-1}{(t-1)/2} (v-1)^{(t+1)/2}.$$

2 The link to codes and resilient functions

It is well-known (see [5]) that an orthogonal array $OA_\lambda(t,n,v)$ is equivalent with a v-ary code of length n with $M = \lambda \cdot v^t$ code-words and dual distance $d' > t$. In the language of coding-theory our bound in Theorem 1 may be expressed as follows:

Theorem 3 *If a v-ary code has length n and M code-words, then its dual distance d' satisfies*
$$d' \leq \frac{v-1}{v} \frac{v^n}{v^n - M} \cdot n.$$

In the case of linear codes this coincides with the Plotkin bound for the dual code. We may therefore interpret our bound as the dual of the Plotkin bound. Meanwhile D.R.Stinson and K.Gopalakrishnan (private communication) have shown that the bound follows from the linear programming-bound. Resilient functions were introduced independently in [1] and [4]. This concept has found numerous applications in cryptography and complexity theory.

Definition 1 *A* **resilient function** *with parameters* (n,m,t) *is a (surjective) function* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$ *such that for every* $v \in \mathbb{F}_2^m$ *the inverse image* $f^{-1}(v)$ *is an orthogonal array* $OA_{2^{n-m-t}}(t,n,2)$.

Thus bounds on orthogonal arrays also yield bounds on resilient functions. Assume a resilient function (n,m,t) exists. Apply Theorem 1 in the binary case (the Friedman bound) to an $OA_{2^{n-m-t}}(t,n,2)$. As $b = 2^{n-m}$ we get $1 \geq 2^m(1 - \frac{n}{2(t+1)})$. Solving for t we get $t \leq \frac{2^{m-1}n}{2^m-1} - 1$:

Corollary 2 *If a resilient function* (n,m,t) *exists, then*

$$t \leq \lfloor \frac{2^{m-1}n}{2^m - 1} \rfloor - 1.$$

References

[1] C.H. Bennett,G.Brassard and J.M.Robert: *Privacy amplification by public discussion,* SIAM J.Comput.17 (1988),210-229.

[2] T.Beth,D.Jungnickel,H.Lenz: *Design Theory,* Bibliographisches Institut, Zürich 1985.

[3] K.A.Bush: *Orthogonal arrays of index unity,* Ann.Math.Stat. 23(1952),426-434.

[4] B.Chor,O.Goldreich,J.Håstad,J.Friedman,S.Rudich and R.Smolensky: *The bit extraction problem or t-resilient functions,* Proc. 26th Symp. on Foundations of Computer Science (1985),396-407.

[5] P.Delsarte: *Four fundamental parameters of a code and their combinatorial significance,* Information and Control 23 (1973),407-438.

[6] J.Friedman: *On the bit extraction problem,* Proc.33rd IEEE Symposium on Foundations of Computer Science (1992),314-319.

[7] C.R.Rao: *Factorial experiments derivable from combinatorial arrangements of arrays,* J.Royal Stat.Soc.9(1947),128-139.