JCD File: 188

Orthogonal Arrays of Strength 3

DONALD L. KREHER

Department of Mathematical Sciences, Michigan Technological University, Houghton, Michigan, U.S.A. 49931–1295

Abstract A new construction for orthogonal arrays of strength 3 is given.

1 Introduction

An *orthogonal array of size* N, *degree* k, *order* s and *strength* t is a k by N array with entries from a set of $s \geq 2$ symbols, having the property that in every t by N subarray, every t by 1 column array appears the same number $\lambda = \frac{N}{s^t}$ times. We denote such an array by $\mathrm{OA}_\lambda(t,k,s)$. The parameter λ is called the *index* of the array.

Existence results for orthogonal arrays of strength greater than or equal to three are few and far between. A summary of these results is given in [3]. For $t = 3$, the best known upper bound on k for fixed λ and s is the Bose-Bush bound [2]:

$$k \leq \left\lfloor \frac{\lambda s^2 - 1}{s-1} - 1 \right\rfloor.$$

A improvement is obtained when $\lambda - 1 \equiv b \pmod{s-1}$ and $1 < b < s-1$:

$$k \leq \left\lfloor \frac{\lambda s^2 - 1}{s-1} \right\rfloor - \left\lfloor \frac{\sqrt{1+4s(s-1-b)} - (2s-2b-1)}{2} \right\rfloor.$$

In [5] orthogonal arrays of strength 2 were constructed by applying a 2-transitive group to certain matrices arising from resolvable linear spaces. This construction motivates the use of 3-transitive groups and resolvable 3-designs to form orthogonal arrays of strength 3. Indeed such a construction is possible and in section 2 we give some new families of strength 3 orthogonal arrays.

2 A new construction

A t–(v,k,λ) *design* is a pair $(X,\mathcal{B})$ where X is a v–element set of *points* and $\mathcal{B}$ is a collection of k–element subsets of X called *blocks* such that every t–element subset of points in contained in exactly λ blocks. A *parallel class* in a t–(v,k,λ) design $(X,\mathcal{B})$ with $v = wk$ is a collection of w disjoint blocks. If $\mathcal{B}$ can be partitioned into parallel classes we say that the design is *resolvable*. There are $r = \lambda\binom{wk-1}{t-1}/\binom{k-1}{t-1}$ parallel classes in such a partition. Thus if the t-(v,k,λ) design $(X,\mathcal{B})$ is resolvable we can construct a w by r matrix A whose entries are the blocks in $\mathcal{B}$ and whose columns are parallel classes. We will call A a *resolution matrix* for $(X,\mathcal{B})$.

It is well known that for $i+j \le t$ the number b_i^j of blocks containing a given set of i points and none of a disjoint set of j points is given by

$$b_i^j = \frac{\binom{v-i-j}{k-i}\lambda}{\binom{v-t}{k-t}}.$$

A permutation group G on Ω is said to be 3-*transitive* if for every pair of 3-tuples $(\alpha_1,\alpha_2,\alpha_3)$ and $(\beta_1,\beta_2,\beta_3)$ there is $g \in G$ that sends α_i to β_i, $i = 1,2,3$. If there is a unique such $g \in G$ for every pair of 3-tuples we say that G acts *sharply* 3-*transitively* on Ω. In this case $|G| = n^3 - n$ where $n+1 = |\Omega|$. The only sharply 3-transitive groups have n a prime power and for every such n, $\mathrm{PGL}_2(n)$ acts sharply 3-transitive on the projective line $\mathrm{GF}(n) \cup \{\infty\}$.

Theorem 2.1 *Let G act 3-transitively on the $(n+1)$-element set Ω and let $m(n^3-n)$ be the order of G. If a resolvable* 3-(wk,k,λ) *design $(X,\mathcal{B})$ exists such that $n = (r-\lambda)/b_2^1 - 2$ with $w-1 \le n \le b_2^1/\lambda$, then an $OA_{mb_2^1(n-1)}(3,wk,n+1)$ also exists.*

Proof. Let $(X,\mathcal{B})$ be a resolvable 3-(wk,k,λ) design with resolution matrix A and define M to be the v by r matrix with entries in $\Omega=\{\omega_1,\omega_2,\ldots,\omega_{n+1}\}$ given by

$$M[i,j]=\omega_k \text{ if and only if } x_i\in A[k,j];$$

where $X=\{x_1,x_2,\ldots,x_v\}$. If $g\in G$, then M^g denotes the matrix obtained by applying g to each of the entries in M. Lastly let C be a v by $(b_2^1(n-1)-\lambda n(n-1))m(n+1)$ matrix with $m(b_2^1(n-1)-\lambda n(n-1))$ constant columns with value ω for each ω in Ω. We claim that the array

$$[M^G,C]=[M^{g_1},M^{g_2},\ldots,M^{g_{|G|}},C], \tag{*}$$

where $G=\{g_1,g_2,\ldots,g_{|G|}\}$, is an $\mathrm{OA}_{mb_2^1(n-1)}(3,v,n+1)$. To see this consider any 3 rows. On these rows there are three types of columns $\begin{bmatrix} x\\ y\\ z\end{bmatrix}$: (i) $x=y=z$, (ii) $x=y\neq z$, (iii) $x=z\neq y$, (iv) $y=z\neq x$ and (v) $x\neq y\neq z\neq x$.

A column of type (i) occurs on these three rows λ times in M and $m(b_2^1(n-1)-\lambda n(n-1))$ times in C. Thus columns of this type occur $\frac{|G|}{n+1}\lambda+m(b_2^1(n-1)-\lambda n(n-1))=mb_2^1(n-1)$ times in array (*) for each such choice of x,y and z.

A column of type (ii) (or of type (iii) or type (iv)) occurs b_2^1 times in M and never in C. Thus such a column occurs $\frac{|G|}{(n+1)n}b_2^1=mb_2^1(n-1)$ times in array (*) for each such choice of x,y and z.

A column of type (v) occurs $r-\lambda-3b_2^1$ times in M and never in C. Thus such a column occurs $\frac{|G|}{(n+1)n(n-1)}(r-\lambda-3b_2^1)=m(r-\lambda-3b_2^1)=mb_2^1(n-1)$ times in array (*) for each such choice of x,y and z. $\square$

The best results are of course obtained when the group G in Theorem 2.1 is sharply 3-transitive. In this case $m=1$ and n is some prime power q. Applying this to resolvable Steiner quadruple systems we obtain Theorem 2.2.

Corollary 2.2 *Let q be a prime power, $q \equiv 1, 5, 9 \pmod{12}$. Then there exists an $OA_{(3q+1)(q-1)/2}(3, 3q+5, q+1)$, except possibly for $q = 197$ or 773.*

Proof. Set $v = 3q + 5$, then $v \equiv 8 \pmod{12}$ and there exists a resolvable SQS(v) (see [4]), i.e. a resolvable 3–$(v, 4, 1)$ design with $w = \frac{v}{4} = \frac{3q+5}{4}$, $r = (v-1)(v-2)/6 = (3q+4)(q+1)/2$ and $b_2^1 = \frac{v-4}{2} = \frac{3q+1}{2}$. Thus $w - 1 \leq q \leq b_2^1$ holds and furthermore $q = (r-1)/b_2^1 - 2$. The result now follows from Theorem 2.1. □

The only other block size we know of for which general existence results are known are the resolvable 3–$(v, 3, 1)$ designs. These exist according to Baranyai's result [1] if and only if $v \equiv 0 \pmod{3}$.

Corollary 2.3 *Let q be a prime power, $q \equiv 1 \pmod{3}$. Then there exists an $OA_{(2q+1)(q-1)}(3, 2q+4, q+1)$.*

Proof. Set $v = 2q+4$, then $v \equiv 0 \pmod{3}$ and there exists by [1] a resolvable 3–$(v, 3, 1)$ design with $w = \frac{v}{3} = \frac{2q+4}{3}$, $r = (v-1)(v-2)/2 = (2q+3)(q+1)$ and $b_2^1 = v - 3 = 2q + 1$. Thus $w - 1 \leq q \leq b_2^1$ holds and furthermore $q = (r-1)/b_2^1 - 2$. The result now follows from Theorem 2.1. □

Acknowledgments

The author is grateful to C.J. Colbourn for his careful reading of an earlier version of this article.

Bibliography

1. Z. Baranyai, On the factorization of the complete uniform hypergraph, *Coll. Math. Soc. Janos Bolyai* **10** (1975), 91-108.

2. R.C. Bose and K.A. Bush, Orthogonal arrays of strength two and three, *Ann. Math. Stat.* **23** (1952), 508-524.

3. J. Bierbrauer and C.J. Colbourn, "Orthogonal arrays of strength more than two", *The CRC handbook of Combinatorial Designs*, C.J. Colbourn and J.H. Dinitz) (Editors), CRC Press, Boca Raton, 1996.

4. A. Hartman and K.T. Phelps, Steiner Quadruple Systems, in *Contemporary Design Theory: A collection of Surveys*, J.H. Dinitz and D.R. Stinson Eds., Wiley, 1992.

5. C.J. Colbourn and D.L. Kreher, Concerning difference matrices, *Designs, Codes and Cryptography*, to appear.