Affine designs and linear orthogonal arrays ⋆

Vladimir D. Tonchev

Department of Mathematical Sciences, Michigan Technological University, Houghton, Michigan 49931, USA, tonchev@mtu.edu

Abstract

It is proved that the collection of blocks of an affine 1-design that yields a linear orthogonal array is a union of parallel classes of hyperplanes in a finite affine space. In particular, for every prime power q and every $m \geq 2$ there exists a unique (up to equivalence) complete linear orthogonal array of strength two associated with the classical design of points and hyperplanes in $AG(m, q)$.

Key words: affine design, affine geometry, orthogonal array, linear code
1991 MSC: 05B, 51E, 94B

1 Introduction

A *design* $D = (X, B)$ is a collection B of subsets (called *blocks*) of a given *point* set X [1]. A t-(v, k, λ) design has blocks of size k on a set of v points, and every t points are contained in exactly λ blocks.

A *parallel class* in a design with blocks of size k and $v = qk$ points is a collection of q pairwise disjoint blocks that partition the point set X.

An 1-(qk, k, r) design is *resolvable* if its collection of blocks can be partitioned into r disjoint parallel classes.

An *affine* design is a resolvable 1-(qk, k, r) design such that every two blocks that belong to different parallel classes share exactly μ points. It follows that an affine design has $v = |X| = q^2\mu$ points, block size $k = q\mu$, and $b = |B| = qr$ blocks. Thus, the parameters of an affine design are of the form 1-$(q^2\mu, q\mu, r)$.

⋆ Research sponsored by the National Security Agency under Grant MDA904-03-1-0088, and NSF Grant CCR-0310832.

An *orthogonal array* $A = OA_t(q, n, \mu)$ of strength t with q distinct symbols, n columns (or *constraints*), and index μ, is a $q^t\mu \times n$ matrix A with entries from a set F_q of size q such that every submatrix consisting of t distinct columns of A contains every ordered t-tuple $(\alpha_1, \ldots, \alpha_t) \in F_q^t$ exactly μ times as a row. Any orthogonal array $OA_t(q, n, \mu)$ is also an orthogonal array of strength s for any $s < t$, with index $\mu_s = q^{t-s}\mu$.

Shrikhande and Bhagwandas [10], [9] proved that an orthogonal array of strength one, $OA_1(q, n, \mu_1)$, exists if and only if a resolvable 1-(v, k, r) design exists with $v = q\mu_1$ points, block size $k = \mu_1$, and $r = n$ parallel classes. Similarly, an orthogonal array of strength two, $OA_2(q, n, \mu)$, exists if and only if an affine 1-$(q^2\mu, q\mu, n)$ design exists. The correspondence between an orthogonal array A and the related resolvable design D is straightforward: the points of D are labeled by the rows of A, and every column of A corresponds to a parallel class of D. The q parallel blocks corresponding to a column of A are labeled by the q different symbols in that column.

Bose and Bush [2] proved the following upper bound on the number of constraints in an orthogonal array of strength two:

$$n \leq \frac{q^2\mu - 1}{q - 1}.$$

An orthogonal array with $n = (q^2\mu - 1)/(q - 1)$ is called *complete*. An orthogonal array $OA_2(q, n, \mu)$ is complete if and only if the corresponding affine 1-$(q^2\mu, q\mu, n)$ design is a 2-$(q^2\mu, q\mu, (q\mu - 1)/(q - 1))$ design [2], [7], [8].

Two orthogonal arrays with the same parameters are *equivalent* if one can be obtained from the other by permutations of the columns, the rows, and the symbols in each column.

A q-ary *code* of length n is a set of n-tuples (or vectors) with components from a finite set of size q. A *linear* q-ary code C of length n is a linear subspace of $GF(q)^n$, where q is a prime power. The *dual* code $C^\perp$ is defined as the orthogonal space of C with respect to the ordinary scalar product in $GF(q)^n$.

An orthogonal array with n columns and q symbols from a finite field $GF(q)$ is *linear* if its rows form a linear subspace of $GF(q)^n$, or in other words, if the rows of the array form a linear q-ary code of length n. Note that any linear code over $GF(q)$ with dual Hamming distance $d^\perp$ is a linear orthogonal array of strength $d^\perp - 1$.

The goal of this note is to characterize the affine designs related to linear orthogonal arrays of strength two. It is proved that the collection of blocks of an affine design that yields a linear orthogonal array is a union of parallel classes of hyperplanes in a finite affine space. In addition, for any prime power

q and any $m \geq 2$ there exists a unique (up to equivalence) complete linear orthogonal array of strength two and $n = (q^m - 1)/(q - 1)$ constraints, and the affine design associated with this array is the classical design of points and hyperplanes in $AG(m, q)$.

2 Linear orthogonal arrays of strength two

We consider arrays with entries from a finite field of order q. In order an orthogonal array to be linear it is necessary that one of the rows is the all-zero row. This can be achieved by permuting the symbols in each of the columns. Hence, every orthogonal array with symbols from $GF(q)$ is equivalent to an array that contains the all-zero row. In addition, the number of rows $q^2\mu$ must be a power of q, hence μ is a power of q. Thus, if A is a linear orthogonal array of strength two with n columns and q^m rows, its index is $\mu = q^{m-2}$. Consequently, the parameters of the affine design associated with A are 1-(q^m, q^{m-1}, n) for some $m \geq 2$.

Theorem 1 *The collection of blocks of any affine 1-(q^m, q^{m-1}, n) design D that corresponds to a linear orthogonal array of strength two $A = OA_2(q, n, q^{m-2})$ over $GF(q)$ is a union of parallel classes of hyperplanes in the m-dimensional affine space $AG(m, q)$.*

Proof. Let $g_1, \ldots, g_m$ be m linearly independent rows of a linear orthogonal array A with q^m rows. Every row $x = (x_1, \ldots, x_n)$ of A is a unique linear combination of $g_1, \ldots, g_m$:

$$x = \alpha_1 g_1 + \ldots + \alpha_m g_m$$

for some $\alpha_1, \ldots, \alpha_m \in GF(q)$. Thus, we can label the rows of A by the vectors $(\alpha_1, \ldots, \alpha_m) \in GF(q)^m$, or equivalently, by the points of $AG(m, q)$. Let G be the m by n matrix having $g_1, \ldots, g_m$ as rows, and let $(g_{1i}, \ldots, g_{mi})^T$ be the ith column of G $(1 \leq i \leq n)$. Then

$$x_i = \alpha_1 g_{1i} + \ldots \alpha_m g_{mi}.$$

Since the array A does not contain all-zero columns, each column of G is a nonzero vector. It follows that for every $\beta \in GF(q)$, the linear equation

$$\alpha_1 g_{1i} + \ldots \alpha_m g_{mi} = \beta \tag{1}$$

has q^{m-1} solutions $(\alpha_1, \ldots, \alpha_m) \in GF(q)^m$ that form a coset of an $(m-1)$-dimensional vector subspace of $GF(q)^m$, or equivalently, a hyperplane in the m-dimensional affine space $AG(m, q)$. Thus, for every $\beta \in GF(q)$, the labels $(\alpha_1, \ldots, \alpha_m)$ of the q^{m-1} entries in the ith column of A that are equal to β form

a hyperplane in $AG(m,q)$ with equation (1). The q hyperplanes corresponding to the q different values of β are pairwise disjoint and form a parallel class in $AG(m,q)$. □

In the special case when the orthogonal array A is complete, the collection of $n=(q^m-1)/(q-1)$ parallel classes obtained from the columns of A includes all hyperplanes in $AG(m,q)$. Hence, the related design is the classical affine 2-$(q^m, q^{m-1}, (q^{m-1}-1)/(q-1))$ design having as points and blocks the points and hyperplanes in $AG(m,q)$. Thus, we have the following.

Corollary 2 *For every prime power q and every $m \geq 2$, there exists only one, up to equivalence, linear complete orthogonal array $OA_2(q,(q^m-1)/(q-1),q^{m-2})$. The related affine 2-$(q^m, q^{m-1}, (q^{m-1}-1)/(q-1))$ design is isomorphic to the classical design of points and hyperplanes in $AG(m,q)$.*

Proof. The affine 2-$(q^m, q^{m-1}, (q^{m-1}-1)/(q-1))$ designs related to any two linear arrays A_1, A_2 are isomorphic to the classical design in $AG(m,q)$. This implies that the arrays A_1, A_2 are equivalent. □

Remark 3 The unique linear code of length $n=(q^m-1)/(q-1)$ and dimension m that corresponds to a linear complete array $OA_2(q,(q^m-1)/(q-1),q^{m-2})$ is the well known simplex code, or the dual code of the q-ary Hamming code. To see that, it is sufficient to notice that every two columns in an orthogonal array of strength two are linearly independent. Consequently, every two columns in the m by $(q^m-1)/(q-1)$ generator matrix G described in the proof of Theorem 1 are linearly independent, hence G is a parity check matrix of a single-error-correcting perfect linear code, or the q-ary Hamming code.

Remark 4 For any prime power q, the number of nonisomorphic affine 2-designs with parameters

$$v=q^m,\ k=q^{m-1},\ \lambda=\frac{q^{m-1}-1}{q-1}$$

grows exponentially with m (Jungnickel [4], Kantor [5], Lam, Lam and Tonchev [6]). These affine designs yield an exponentially growing number of inequivalent and generally nonlinear complete orthogonal arrays $OA_2(q, n=(q^m-1)(q-1), \mu=q^{m-2})$.

Acknowledgment. The author thanks the referees for their useful remarks.

References

[1] T. Beth, D. Jungnickel, H. Lenz, "Design Theory", Second Edition, Cambridge University Press, Cambridge 1999.

[2] R.C. Bose and K. A. Bush, Orthogonal arrays of strength two and three, *Sankhyă* **6** (1942), 105-110.

[3] A.S. Hedayat, N.J.A. Sloane, John Stufken, "Orthogonal Arrays", Springer, New York 1999.

[4] D. Jungnickel, The number of Designs with classical parameters grows exponentially, *Geometriae Dedicata*, 16(1984), pp. 167–178.

[5] W. M. Kantor, "Automorphisms and Isomorphisms of Symmetric and Affine Designs", *J. Algebraic Combinatorics*, 3(1994), pp. 307–338.

[6] C. Lam, S. Lam, and V. D. Tonchev, Bounds on the number of affine, symmetric and Hadamard designs and matrices, *J. Combinatorial Theory*, Ser. A **92** (2000), 186-196.

[7] V. Mavron, Parallelisms in designs, *J. London Math. Soc.*, Ser. 2 **4** (1972), 682-684.

[8] R.L. Plackett and J.B. Burman, The design of optimum multifactorial experiments, *Biometrika* **33** (1946), 305-325.

[9] S.S. Shrikhande, Affine resolvable balanced incomplete block designs: a survey, *Aequationes Math.* **14** (1976), 251-269.

[10] S.S. Shrikhande and D. Bhagwandas, On embedding of orthogonal arrays of strength two, in: "Combinatorial Mathematica and its applications", edited by R.C. Bose and T.A. Dowling, pp. 256-273, University of North Carolina Press, 1969.