Journal of Statistical Planning and
Inference 115 (2003) 623–635

Construction of asymmetric orthogonal arrays through finite geometries

Chung-yi Suen[a,*], Aloke Dey[b]

[a] *Cleveland State University, Cleveland, OH 44114-4435, USA*
[b] *Indian Statistical Institute, New Delhi 110 016, India*

Abstract

Finite geometries are used to construct several families of asymmetric orthogonal arrays. Many of these arrays appear to be new.

Keywords: Orthogonal arrays; Finite geometry; Tight arrays

1. Introduction

An orthogonal array, $\mathrm{OA}(N, n, m_1 \times \cdots \times m_n, g)$ is an $N \times n$ matrix with symbols in the ith column from a finite set of $m_i(\geqslant 2)$ symbols, $1 \leqslant i \leqslant n$, such that in every $N \times g$ submatrix, all possible combinations of symbols appear equally often as a row. Orthogonal arrays with $m_1 = \cdots = m_n = m$ (say) are called symmetric and we denote such arrays by $\mathrm{OA}(N, n, m, g)$; otherwise, the array is called asymmetric. For the construction and applications of orthogonal arrays in design of experiments, see Hedayat et al. (1999) and Dey and Mukerjee (1999).

It is known that for an $\mathrm{OA}(N, n, m_1 \times \cdots \times m_n, g)$,

$$N \geqslant 1 + \sum_{1 \leqslant i \leqslant n} (m_i - 1) + \sum_{1 \leqslant i_1 < i_2 \leqslant n} (m_{i_1} - 1)(m_{i_2} - 1)$$

$$+ \cdots + \sum_{1 \leqslant i_1 < \cdots < i_u \leqslant n} (m_{i_1} - 1) \cdots (m_{i_u} - 1) \quad \text{if } g(=2u,\ u \geqslant 1) \text{ is even}$$

and

$$N \geqslant 1 + \sum_{1 \leqslant i \leqslant n} (m_i - 1) + \sum_{1 \leqslant i_1 < i_2 \leqslant n} (m_{i_1} - 1)(m_{i_2} - 1)$$

$$+ \cdots + \sum_{1 \leqslant i_1 < \cdots < i_u \leqslant n} (m_{i_1} - 1) \cdots (m_{i_u} - 1)$$

$$+ (m_1 - 1) \sum_{2 \leqslant i_1 < \cdots < i_u \leqslant n} (m_{i_1} - 1) \cdots (m_{i_u} - 1)$$

if $g(=2u+1,\ u \geqslant 1)$ is odd and $m_1 = \max_{1 \leqslant i \leqslant n} m_i$.

Orthogonal arrays for which the number of rows N attains the above lower bounds are called *tight*. Tight orthogonal arrays are of great importance in design of experiments as optimal fractional factorial plans with the least number of runs.

The construction of asymmetric orthogonal arrays of strength *two* have received considerable attention. Asymmetric orthogonal arrays of strengths greater than two have however, received less attention in the literature. The purpose of this communication is to present some methods of construction of asymmetric orthogonal arrays of arbitrary strength. The methods are based on finite projective geometries and we refer the reader e.g., to Hirschfeld (1979, 1985) for an excellent account of finite projective geometries. In Section 2, a recent method of Suen et al. (2001) is used to obtain a family of asymmetric orthogonal arrays of strength $g(\geqslant 2)$. Arrays of strength three obtained through this method appear to be new. Some more families of asymmetric orthogonal arrays of strength three and four are presented in Section 3. Several of such arrays also appear to be new.

2. A general method

For m a prime or prime power, let GF(m) denote a Galois field of order m. For completeness, we first state a result of Suen et al. (2001).

Theorem 2.1. *Let C be an $r \times n$ matrix with entries from* GF(m) *and suppose C is written as $C = [F_1 \vdots \cdots \vdots F_u]$, where for $1 \leqslant i \leqslant u$, F_i is an $r \times n_i$ matrix, $\sum_{i=1}^{u} n_i = n$. If for every choice of g matrices $F_{i_1}, \ldots, F_{i_g}$ out of $F_1, \ldots, F_u$, the $r \times \sum_{j=1}^{g} n_{i_j}$ matrix $[F_{i_1} \vdots \cdots \vdots F_{i_g}]$ has full column rank over* GF(m), *then one can construct an* OA(m^r, $u, (m^{n_1}) \times \cdots \times (m^{n_u}), g$).

The orthogonal array of Theorem 2.1 is given by the row space of C, where the n_i columns of F_i form a new column of m^{n_i} symbols for $1 \leqslant i \leqslant u$. We shall now present a method based on Theorem 2.1 to obtain some families of asymmetric orthogonal arrays. The main result that follows uses a replacement procedure similar to the one employed by Suen et al. (2001). We start with a generating matrix over GF(m^k) and on replacing each entry of the generating matrix by its matrix representation over GF(m),

a new generating matrix is obtained. The final orthogonal array is then generated via another matrix obtained by deleting certain rows of the new generating matrix. We have the following result.

Theorem 2.2. *Let m be a prime or prime power and i,k be integers such that $1 \leqslant i \leqslant k$. If there exists an $r \times u$ matrix A with entries from* GF(m^k) *such that*

(i) *any g columns in A are linearly independent over* GF(m^k), *and*
(ii) *there is a row in A which has exactly t zero entries and $u-t$ nonzero entries.*

Then, one can construct an OA($m^{rk-k+i}, u, (m^k)^t \times (m^i)^{u-t}, g$).

Proof. Without loss of generality, one can assume that in the last row of A, the first t entries are zero and the remaining $u-t$ entries are 1. Replace each entry in A by its $k \times k$ matrix representation, the entries in the matrix representation being elements from GF(m). Call the derived $rk \times uk$ matrix C^*. The matrix C^* is obtained in the following manner.

Let ω be a primitive element of GF(m^k) with minimum polynomial $x^k + \alpha_{k-1}x^{k-1} + \cdots + \alpha_1 x + \alpha_0$, where for $0 \leqslant j \leqslant k-1$, $\alpha_j \in$ GF(m). The companion matrix of the minimum polynomial is

$$W = \begin{bmatrix} 0 & 0 & \ldots & 0 & -\alpha_0 \\ 1 & 0 & \ldots & 0 & -\alpha_1 \\ 0 & 1 & \ldots & 0 & -\alpha_2 \\ \vdots & & & & \\ 0 & 0 & \ldots & 1 & -\alpha_{k-1} \end{bmatrix}.$$

Recall that if ω is a primitive element of GF(m^k), then $0, 1, \omega, \omega^2, \ldots, \omega^{s-2}$ are all the elements of GF(m^k), where $s = m^k$. A typical element ω^j of GF(m^k) can be represented by a $k \times k$ matrix W^j with elements from GF(m), with 0 being represented by a $k \times k$ null matrix and 1, by the identity matrix of order k.

Now, for $1 \leqslant j \leqslant u$, let F_j^* be the $rk \times k$ submatrix such that $C^* = [F_1^* \vdots \cdots \vdots F_u^*]$. Then it can be verified that for any choice of $1 \leqslant j_1 < \cdots < j_g \leqslant u$, the $rk \times gk$ submatrix has full column rank, gk.

Given $1 \leqslant i \leqslant k$, for $t+1 \leqslant j \leqslant u$, let F_j be the $(rk-k+i) \times i$ matrix obtained by deleting the last $k-i$ columns and the last $k-i$ rows of F_j^*, and let for $1 \leqslant j \leqslant t$, F_j be the $(rk-k+i) \times k$ matrix obtained by deleting the last $k-i$ rows of F_j^*. Then the $(rk-k+i) \times (tk+ui-ti)$ matrix $C = [F_1 \vdots \cdots \vdots F_u]$ satisfies the condition of Theorem 2.1, namely, that for any choice of $1 \leqslant j_1 < \cdots < j_g \leqslant u$, the matrix $C_g = [F_{j_1} \vdots \cdots \vdots F_{j_g}]$ has full column rank; this follows because C_g is obtained from $[F_{j_1}^*, \cdots F_{j_g}^*]$ by deleting some columns and then some zero rows. It follows now that the OA($m^{rk-k+i}, u, (m^k)^t \times (m^i)^{u-t}, g$) can be constructed via Theorem 2.1. □

To illustrate Theorem 2.2, we construct a *tight* array OA$(256, 10, 8^2 \times 4^8, 3)$, which appears to be *new*.

Example 2.1. Let $m=2$, $k=3$, $i=2$. Let ω be a primitive element of GF(8) with the minimum polynomial x^3+x+1. The following 3×10 matrix A has the property that any three of its columns are linearly independent over GF(8).

$$A=\begin{bmatrix} 1 & 0 & 0 & 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 \\ 0 & 1 & 0 & 1 & \omega^2 & \omega^4 & \omega^6 & \omega & \omega^3 & \omega^5 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

The companion matrix of the minimum polynomial x^3+x+1 is

$$W=\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

and the elements of GF(8) can be represented by 3×3 matrices with entries from GF(2) as

$$0 \equiv \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad 1 \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \omega \equiv \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \omega^2 \equiv \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix},$$

$$\omega^3 \equiv \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \quad \omega^4 \equiv \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}, \quad \omega^5 \equiv \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}, \quad \omega^6 \equiv \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Replacing each entry in A by its matrix representation, we obtain the matrix C^* as

F_1^*	F_2^*	F_3^*	F_4^*	F_5^*	F_6^*	F_7^*	F_8^*	F_9^*	F_{10}^*
100	000	000	100	001	010	101	011	111	110
010	000	000	010	101	011	111	110	100	001
001	000	000	001	010	101	011	111	110	100
000	100	000	100	010	011	110	001	101	111
000	010	000	010	011	110	001	101	111	100
000	001	000	001	101	111	100	010	011	110
000	000	100	100	100	100	100	100	100	100
000	000	010	010	010	010	010	010	010	010
000	000	001	001	001	001	001	001	001	001

Deleting the last row of C^* and the third column of each of $F_3^*,\ldots,F_{10}^*$, the 8×22 matrix C is obtained, which can now be used to get the $\mathrm{OA}(256,10,8^2\times 4^8,3)$ via Theorem 2.1. □

We now use Theorem 2.2 to construct some specific families of asymmetric orthogonal arrays of strengths two and three. In order to obtain the $r\times u$ matrix A in Theorem 2.2, we make use of points, lines, planes, flats, ovals and ovaloids in a finite projective geometry. A column of A corresponds to a point in the finite projective geometry $\mathrm{PG}(r-1,m^k)$. To construct an array of strength two, any two columns of A must correspond to two distinct points in $\mathrm{PG}(r-1,m^k)$. Similarly, for constructing an array of strength three, any three columns of A must correspond to three noncollinear points of $\mathrm{PG}(r-1,m^k)$. Let us first consider arrays of strength two. To that end, we have the following result.

Theorem 2.3. *Let m be a prime or a prime power and i,k and r be integers such that $1\leqslant i\leqslant k$ and $r\geqslant 2$. Then a tight $\mathrm{OA}(m^{rk-k+i},v_1+v_2,(m^k)^{v_1}\times(m^i)^{v_2},2)$ can be constructed, where $v_1=(m^{rk-k}-1)/(m^k-1)$ and $v_2=m^{rk-k}$.*

Proof. Let A be the $r\times(m^{rk}-1)/(m^k-1)$ matrix such that the columns of A correspond to all the points in $\mathrm{PG}(r-1,m^k)$. Out of these, the $(m^{rk-k}-1)/(m^k-1)$ columns with the last entry zero forms an $(r-2)$-flat. Hence, the last row of A has exactly v_1 zero entries and v_2 nonzero entries. Using Theorem 2.2, the required orthogonal array can now be constructed. □

We now consider arrays of strength three. Most of the arrays constructed below appear to be new.

Theorem 2.4. *Let m be a prime or a prime power and i,k be integers, $1\leqslant i\leqslant k$. Then one can construct*
(a) *a tight $\mathrm{OA}(m^{2k+i},m^k+2,(m^k)^2\times(m^i)^{m^k},3)$, where m is even;*
(b) *an $\mathrm{OA}(m^{2k+i},m^k+1,(m^k)^2\times(m^i)^{m^k-1},3)$, where m is odd.*

Proof. Let the points of the finite projective geometry $\mathrm{PG}(2,m^k)$ be denoted by 3×1 vectors with entries from $\mathrm{GF}(m^k)$. An oval in $\mathrm{PG}(2,m^k)$ has m^k+2 points when m is even and m^k+1 points when m is odd. Any three points on an oval are not collinear. If A be the matrix whose columns are points of an oval in $\mathrm{PG}(2,m^k)$, then it follows that any three columns of A are linearly independent. Moreover, one can assume without loss of generality that the first two columns of A are $(1,0,0)'$ and $(0,1,0)'$. Then the line through the points $(1,0,0)'$ and $(0,1,0)'$ does not meet any other point in the oval, and the points on this line are represented by 3×1 vectors with the last entry equal to zero. It follows then that the last row of A has precisely two zero entries. The required arrays (a) and (b) can now be constructed via Theorem 2.2. □

Remark 2.1. With $i = 1$ in Theorem 2.4, we have the arrays

(i) $\mathrm{OA}(m^{2k+1}, m^k + 2, (m^k)^2 \times m^{m^k}, 3)$ whenever m is even, and
(ii) $\mathrm{OA}(m^{2k+1}, m^k + 1, (m^k)^2 \times m^{m^k - 1}, 3)$, whenever m is odd.

Array (i) was constructed by Suen et al. (2001) through a different technique. Array (ii) is an improvement over a result of Suen et al. (2001) in terms of having more m symbol columns. Note that the array of Example 2.1 is a special case of Theorem 2.4 with $m = 2 = i, k = 3$.

We next have the following result.

Theorem 2.5. *Let m, i, k be as in Theorem* 2.4. *Then one can construct an* $\mathrm{OA}(m^{3k+i}, m^{2k} + 1, (m^k)^{m^k+1} \times (m^i)^{m^{2k}-m^k}, 3)$.

Proof. Let the points of a $\mathrm{PG}(3, m^k)$ be denoted by 4×1 vectors with entries from $\mathrm{GF}(m^k)$. An ovaloid in $\mathrm{PG}(3, m^k)$ has $m^{2k} + 1$ points and any three of these points are not collinear. Any plane in $\mathrm{PG}(3, m^k)$ meets an ovaloid in either one point or, $m^k + 1$ points. If A is the $4 \times (m^{2k} + 1)$ matrix with columns corresponding to the points of an ovaloid, then clearly any three columns of A are linearly independent. Without loss of generality, we can assume that the first three columns of A are $(1,0,0,0)', (0,1,0,0)'$ and $(0,0,1,0)'$. The plane through these points must meet the ovaloid in $m^k + 1$ points, and each of these points has the last entry zero. It follows then that the last row of A has exactly $m^k + 1$ zero entries and $m^{2k} - m^k$ nonzero entries. The result now follows from Theorem 2.2. □

As an application of Theorem 2.5, let $m = 2 = k, i = 1$. We then have the array $\mathrm{OA}(128, 17, 4^5 \times 2^{12}, 3)$. This array, however is not tight. It is not known whether a tight array $\mathrm{OA}(128, 24, 4^5 \times 2^{19}, 3)$ exists or not.

3. Some more orthogonal arrays

Suen et al. (2001) constructed the following arrays:

(i) $\mathrm{OA}(m^5, m^2 + m + 2, (m^2) \times m^{m^2+m+1}, 3)$, where m is an *even* prime power, and
(ii) $\mathrm{OA}(m^5, m + 2, (m^2) \times m^{m+1}, 4)$, where m is a prime or a prime power.

In this section, we improve these results by constructing the following families of arrays:

(i′) $\mathrm{OA}(m^5, m^2 + m + 2, (m^2) \times m^{m^2+m+1}, 3)$, where m is a prime or a prime power, and
(ii′) $\mathrm{OA}(m^5, m + 3, (m^2) \times m^{m+2}, 4)$, where m is an even prime power.

Note that the array (i′) is tight. Although the array (ii′) is not tight, one can show that in an $\mathrm{OA}(m^5, n+1, (m^2) \times m^n, 4)$, $n \leqslant m+2$. To see this, suppose an $\mathrm{OA}(m^5, n+1, (m^2) \times m^n, 4)$ exists. Then deleting the first column of the $m^3 \times (n+1)$ subarray given by rows with the same symbol in the first column, one gets a symmetric $\mathrm{OA}(m^3, n, m, 3)$.

By a result of Bush (1952), in a symmetric OA($m^3, n, m, 3$), $n \leqslant m+1$ if m is odd and, $n \leqslant m+2$, if m is even. It follows that if m is an even prime power then in an OA($m^5, n+1, (m^2) \times m^n, 4$), $n \leqslant m+2$.

For constructing the arrays (i′) and (ii′), the following preliminaries will be helpful. Recall that in a finite projective geometry, PG($r-1, m$) of dimension $r-1$, a point is an ordered r-tuple $(x_0, x_1, \ldots, x_{r-1})$, $x_i \in \mathrm{GF}(m)$, $0 \leqslant i \leqslant r-1$. Two such vectors $(x_0, x_1, \ldots, x_{r-1})$ and $(y_0, y_1, \ldots, y_{r-1})$ represent the same point if there exists a $\lambda \neq 0$ such that for $0 \leqslant i \leqslant r-1$, $x_i = \lambda y_i$. An elliptic quadric in PG($3, m$) consists of m^2+1 points such that any three points are not collinear. It has the following canonical form (see e.g., Hirschfeld (1979, Theorem 5.2.4):

$$x_0 x_1 = f(x_2, x_3),$$

where f is an irreducible binary quadratic form. We then have the following

Lemma 3.1. *Let* $V = \{(1, f(y,z), y, z) : y, z \in \mathrm{GF}(m)\}$ be a set of m^2 *vectors, each of order* 1×4, *where* f *is an irreducible binary quadratic form. Then any three vectors in* V *are linearly independent.*

Proof. The result follows since V contains m^2 points of the elliptic quadric $x_0 x_1 = f(x_2, x_3)$ in PG($3, m$) (the other point not in V is (0,1,0,0)). □

We now have the following result.

Theorem 3.1. *An* OA($m^5, m^2+m+2, (m^2) \times m^{m^2+m+1}, 3$) *can be constructed for any prime or prime power* m.

Proof. The required array can be constructed if we can find a matrix C of order $5 \times (m^2+m+3)$, satisfying the condition of Theorem 2.1. Let $C = [F_1 \vdots \cdots \vdots F_{m^2+m+2}]$, where

$$F_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}, \quad F_2 = [1 \quad 0 \quad 0 \quad 0 \quad 1]',$$

$$F_i = [1 \quad x^2 \quad 0 \quad 1 \quad x]', \quad 1 \leqslant i \leqslant m+2, \ x \in \mathrm{GF}(m)$$

and

$$F_j = [0 \quad f(y,z) \quad 1 \quad y \quad z]', \quad m+3 \leqslant j \leqslant m^2+m+2, \ y, z \in \mathrm{GF}(m),$$

$f(y,z)$ is irreducible.

With the above choices of the matrices F_i, $1 \leqslant i \leqslant m^2+m+2$, we now show by considering all possible cases that the rank condition of Theorem 2.1 is met.

(1) Let $i=1$, $j=2$, $3 \leqslant k \leqslant m+2$. The matrix $[F_1 \vdots F_2 \vdots F_k]$ must have rank 4. Now,

$$[F_1 \vdots F_2 \vdots F_k] = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & x^2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & x \end{bmatrix}.$$

The above matrix has rank 4 since the determinant of the 4×4 submatrix given by the first, second, fourth and fifth rows equals -1.

(2) Let $i=1$, $j=2$, $m+3 \leqslant k \leqslant m^2+m+2$. The matrix $[F_1 \vdots F_2 \vdots F_k]$ must have rank 4. Now,

$$[F_1 \vdots F_2 \vdots F_k] = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & f(y,z) \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & y \\ 0 & 0 & 1 & z \end{bmatrix}.$$

The above matrix has rank 4 since the determinant of the 4×4 submatrix given by the first, second, third and fifth rows equals -1.

(3) Let $i=1$, $3 \leqslant j < k \leqslant m+2$. The matrix $[F_1 \vdots F_j \vdots F_k]$ must have rank 4. We have

$$[F_1 \vdots F_j \vdots F_k] = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & x_1^2 & x_2^2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & x_1 & x_2 \end{bmatrix}.$$

The above matrix has rank 4 since the determinant of the 4×4 submatrix given by the first, second, fourth and fifth rows equals $x_2 - x_1 \neq 0$.

(4) Let $i=1$, $3 \leqslant j \leqslant m+2$, $m+3 \leqslant k \leqslant m^2+m+2$. The matrix $[F_1 \vdots F_j \vdots F_k]$ must have rank 4. We have

$$[F_1 \vdots F_j \vdots F_k] = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & x^2 & f(y,z) \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & y \\ 0 & 0 & x & z \end{bmatrix}.$$

The above matrix has rank 4 since the determinant of the 4×4 submatrix given by the first four rows equals $-1 \neq 0$.

(5) Let $i=1$, $m+3 \leqslant j < k \leqslant m^2+m+2$. The matrix $[F_1 \vdots F_j \vdots F_k]$ must have rank 4. In this case,

$$[F_1 \vdots F_j \vdots F_k] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & f(y_1,z_1) & f(y_2,z_2) \\ 0 & 0 & 1 & 1 \\ 0 & 0 & y_1 & y_2 \\ 0 & 0 & z_1 & z_2 \end{bmatrix} \quad \text{where } (y_1,z_1) \neq (y_2,z_2).$$

If $y_1 \neq y_2$, the determinant of the 4×4 submatrix formed by the first four rows equals $y_2 - y_1 \neq 0$. If $z_1 \neq z_2$,the determinant of the 4×4 submatrix formed by the first, second, third and fifth rows equals $z_2 - z_1 \neq 0$ and thus, in either case, the rank of $[F_1 \vdots F_j \vdots F_k]$ is 4.

(6) Let $i = 2$, $3 \leqslant j < k \leqslant m+2$. The matrix $[F_2 \vdots F_j \vdots F_k]$ must have rank 3. In this case,

$$[F_2 \vdots F_j \vdots F_k] = \begin{bmatrix} 1 & 1 & 1 \\ 0 & x_1^2 & x_2^2 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & x_1 & x_2 \end{bmatrix} \quad \text{where } x_1 \neq x_2.$$

$[F_2 \vdots F_j \vdots F_k]$ has rank 3 since the determinant of the 3×3 submatrix formed by the first, fourth and fifth rows equals $x_2 - x_1 \neq 0$.

(7) Let $i = 2$, $3 \leqslant j \leqslant m+2$, $m+3 \leqslant k \leqslant m^2+m+2$. The matrix $[F_2 \vdots F_j \vdots F_k]$ must have rank 3. In this case,

$$[F_2 \vdots F_j \vdots F_k] = \begin{bmatrix} 1 & 1 & 0 \\ 0 & x^2 & f(y,z) \\ 0 & 0 & 1 \\ 0 & 1 & y \\ 1 & x & z \end{bmatrix}.$$

This matrix has rank 3 since the determinant of the 3×3 submatrix formed by the last three rows equals $-1 \neq 0$.

(8) Let $i=2$, $m+3 \leqslant j < k \leqslant m^2+m+2$. The matrix $[F_2 \vdots F_j \vdots F_k]$ must have rank 3. Here,

$$[F_2 \vdots F_j \vdots F_k] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & f(y_1,z_1) & f(y_2,z_2) \\ 0 & 1 & 1 \\ 0 & y_1 & y_2 \\ 1 & z_1 & z_2 \end{bmatrix} \quad \text{where } (y_1,z_1) \neq (y_2,z_2).$$

If $y_1 \neq y_2$, the determinant of the 3×3 submatrix formed by the last three rows equals $y_2 - y_1 \neq 0$. If $z_1 \neq z_2$, the determinant of the 3×3 submatrix formed by the first, third and fifth rows equals $z_2 - z_1 \neq 0$ and thus, in either case, the rank of $[F_2 \vdots F_j \vdots F_k]$ is 3.

(9) Let $3 \leqslant i < j < k \leqslant m+2$. The matrix $[F_i \vdots F_j \vdots F_k]$ must have rank 3. In this case,

$$[F_i \vdots F_j \vdots F_k] = \begin{bmatrix} 1 & 1 & 1 \\ x_1^2 & x_2^2 & x_3^2 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \\ x_1 & x_2 & x_3 \end{bmatrix},$$

where x_1, x_2, x_3 are distinct elements of GF(m). $[F_i \vdots F_j \vdots F_k]$ has rank 3 since the determinant of the 3×3 submatrix formed by the first, second and fifth rows equals $-(x_2 - x_1)(x_3 - x_1)(x_3 - x_2) \neq 0$.

(10) Let $3 \leqslant i < j \leqslant m+2$, $m+3 \leqslant k \leqslant m^2+m+2$. The matrix $[F_i \vdots F_j \vdots F_k]$ must have rank 3. Here,

$$[F_i \vdots F_j \vdots F_k] = \begin{bmatrix} 1 & 1 & 0 \\ x_1^2 & x_2^2 & f(y,z) \\ 0 & 0 & 1 \\ 1 & 1 & y \\ x_1 & x_2 & z \end{bmatrix},$$

where x_1, x_2 are distinct elements of GF(m). $[F_i \vdots F_j \vdots F_k]$ has rank 3 since the determinant of the 3×3 submatrix formed by the last three rows equals $x_2 - x_1 \neq 0$.

(11) Let $3 \leqslant i \leqslant m+2$, $m+3 \leqslant j < k \leqslant m^2+m+2$. The matrix $[F_i \vdots F_j \vdots F_k]$ must have rank 3. In this case,

$$[F_i \vdots F_j \vdots F_k] = \begin{bmatrix} 1 & 0 & 0 \\ x^2 & f(y_1,z_1) & f(y_2,z_2) \\ 0 & 1 & 1 \\ 1 & y_1 & y_2 \\ x & z_1 & z_2 \end{bmatrix} \quad \text{where } (y_1,z_1) \neq (y_2,z_2).$$

If $y_1 \neq y_2$, the determinant of the 3×3 submatrix given by the first, third and fourth rows equals $y_2 - y_1 \neq 0$. If $z_1 \neq z_2$, the determinant of the 3×3 submatrix formed by the first, third and fifth rows equals $z_2 - z_1 \neq 0$. Thus, in either case, $[F_i \vdots F_j \vdots F_k]$ has rank 3.

(12) Let $m+3 \leqslant i < j,k \leqslant m^2+m+2$. In this case,

$$[F_i \vdots F_j \vdots F_k] = \begin{bmatrix} 0 & 0 & 0 \\ f(y_1,z_1) & f(y_2,z_2) & f(y_3,z_3) \\ 1 & 1 & 1 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{bmatrix},$$

where $(y_1,z_1),(y_2,z_2)$ and (y_3,z_3) are distinct. The matrix $[F_i \vdots F_j \vdots F_k]$ has rank 3 by Lemma 3.1.

Thus the result is proved. □

We illustrate the above theorem below.

Example 3.1. Let 0,1 and 2 be the elements of GF(3). Then $f(y,z) = y^2 + z^2$ is irreducible over GF(3). An OA$(243, 14, 9 \times 3^{13}, 3)$ can be constructed via Theorem 2.1 using the following matrix C:

$$C = \begin{bmatrix} F_1 & F_2 & F_3 & F_4 & F_5 & F_6 & F_7 & F_8 & F_9 & F_{10} & F_{11} & F_{12} & F_{13} & F_{14} \\ 10 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 01 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 2 & 2 & 1 & 2 & 2 \\ 00 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 00 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 00 & 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}$$

We next construct an OA$(m^5, m+3, (m^2) \times m^{m+2}, 4)$, where m is an even prime power. Suen et al. (2001) constructed an OA$(m^5, m+2, (m^2) \times m^{m+1}, 4)$ for any prime or prime power m. When m is odd, these arrays have the maximum number of m-symbol columns. For even m, the number of m-level columns is at most $m+2$ and we show

that this upper bound on the number of m-level columns can actually be achieved. To that end, we first have the following lemma.

Lemma 3.2. *If m is an even prime power, then there exists an $\alpha \in \mathrm{GF}(m)$ such that $x^2 + x \neq \alpha$ for all $x \in \mathrm{GF}(m)$.*

Proof. For any $x \in \mathrm{GF}(m)$, $(x+1)^2 + x + 1 = x^2 + x$, since m is even. Also, since the set $\{x^2 + x : x \in \mathrm{GF}(m)\}$ contains exactly $m/2$ elements and there are m elements in $\mathrm{GF}(m)$, there exists an $\alpha \in \mathrm{GF}(m)$ such that $x^2 + x \neq \alpha$ for all $x \in \mathrm{GF}(m)$. □

We now have the following result.

Theorem 3.2. *If m is an even prime power, then an $\mathrm{OA}(m^5, m+3, (m^2) \times m^{m+2}, 4)$ can be constructed.*

Proof. Let $C = [F_1 \vdots \cdots \vdots F_{m+3}]$, where

$$F_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}', \quad F_2 = [1\ 1\ 0\ 0\ 1]',$$

$$F_3 = [1\ \alpha\ 0\ 1\ 0]' \quad \text{where } \alpha \neq x^2 + x \text{ for all } x \in \mathrm{GF}(m),$$

and

$$F_i = [0 \quad x^3 \quad 1 \quad x \quad x^2]',\ x \in \mathrm{GF}(m),\ 4 \leqslant i \leqslant m+3.$$

One can show that with above choices for the matrices F_i, $1 \leqslant i \leqslant m+3$, the rank condition of Theorem 2.1 is satisfied. In order to save space, we demonstrate this only in one case; the other cases can be handled in the same way as in the proof of Theorem 3.1.

Let $i = 2, j = 3, 4 \leqslant k < l \leqslant m+3$. Then, the matrix $[F_2 \vdots F_3 \vdots F_k \vdots F_l]$ must have rank 4. Now,

$$[F_2 \vdots F_3 \vdots F_k \vdots F_l] = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & \alpha & x_1^3 & x_2^3 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & x_1 & x_2 \\ 1 & 0 & x_1^2 & x_2^2 \end{bmatrix} \quad \text{where } x_1 \neq x_2.$$

By elementary row operations, this matrix can be shown to be row equivalent to

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & x_1 & x_2 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & (x_1 + x_2)(x_1 + x_2 + 1) \\ 0 & 0 & 0 & (x_1 + x_2)(x_1^2 + x_2^2 + x_1 x_2 + \alpha + 1) \end{bmatrix}$$

Since $x_1+x_2\neq 0$, the above matrix has rank 4 if either $x_1+x_2+1\neq 0$ or, $x_1^2+x_2^2+x_1x_2+\alpha+1\neq 0$. If $x_1+x_2+1=0$, then $x_1^2+x_2^2+x_1x_2+\alpha+1=x_1^2+x_2(x_1+x_2)+\alpha+1=x_1^2+x_1+\alpha\neq 0$ for any $x_1\in \mathrm{GF}(m)$, by the choice of α. Hence x_1+x_2+1 and $x_1^2+x_2^2+x_1x_2+\alpha+1$ cannot be zero simultaneously for any $x_1\neq x_2$. Hence the rank of the matrix is 4. □

We give an example to illustrate Theorem 3.2.

Example 3.2. Let $m=4$ and let $0,1,\omega$ and $\omega^2(=\omega+1)$ be the elements of GF(4). Set $\alpha=\omega\neq x^2+x$ for any $x\in \mathrm{GF}(4)$. An $\mathrm{OA}(4^5,7,16\times 4^6,4)$ can be constructed by choosing the matrix C appearing in Theorem 2.1 as

$$C=\begin{bmatrix} F_1 & F_2 & F_3 & F_4 & F_5 & F_6 & F_7 \\ 10 & 1 & 1 & 0 & 0 & 0 & 0 \\ 01 & 1 & \omega & 0 & 1 & 1 & 1 \\ 00 & 0 & 0 & 1 & 1 & 1 & 1 \\ 00 & 0 & 1 & 1 & 1 & \omega & \omega^2 \\ 00 & 1 & 0 & 0 & 1 & \omega^2 & \omega \end{bmatrix}$$

References

Bush, K.A., 1952. Orthogonal arrays of index unity. Ann. Math. Statist. 23, 426–434.

Dey, A., Mukerjee, R., 1999. Fractional Factorial Plans. Wiley, New York.

Hedayat, A.S., Sloane, N.J.A., Stufken, J., 1999. Orthogonal Arrays: Theory and Applications. Springer, New York.

Hirschfeld, J.W.P., 1979. Projective Geometries Over Finite Fields. Oxford University Press, Oxford.

Hirschfeld, J.W.P., 1985. Finite Projective Spaces of Three Dimensions. Oxford University Press, Oxford.

Suen, C., Das, A., Dey, A., 2001. On the construction of asymmetric orthogonal arrays. Statist. Sinica 11, 241–260.