No. 758

A Construction of Combinatorial arrays from Non-linear Functions

by

Ryoh Fuji-Hara and Nobuko Miyamoto

October 1997

A Construction of Combinatorial arrays from Non-linear Functions

Ryoh Fuji-Hara and Nobuko Miyamoto
(fujihara@sk.tsukuba.ac.jp)
(nmiyamot@sk.tsukuba.ac.jp)

Institute of Policy and Planning Sciences,
University of Tsukuba,
Tsukuba, Ibaraki, Japan 305

Abstract

Bose [2] proposed a construction of orthogonal arrays. The construction uses linear transformations over a finite field. Fuji-Hara and Miyamoto [3] generalized this method by considering non-linear functions in stead of linear transformations and constructed combinatorial arrays such as orthogonal arrays and balanced arrays. In particular, we constructed combinatorial arrays by using quadratic functions over finite fields of even prime power orders. In this paper, we construct combinatorial arrays for odd prime power orders. Moreover we give some constructions of balanced arrays as an application of the results obtained here.

1 Introduction

Let S be a set $\{0, 1, \ldots, s-1\}$ of s symbols and let S^t be the set of all t-dimensional column vectors over S. A *balanced array* of strength t, denoted by $BA(N, k, s, t)$, is a $k \times N$ array $\boldsymbol{A}$ whose elements are from S satisfying the following conditions:

(i) in any t-rowed subarray $\boldsymbol{A}_0$ of $\boldsymbol{A}$, $\boldsymbol{x} \in S^t$ appears $\lambda(\boldsymbol{x})$ times in $\boldsymbol{A}_0$.

(ii) for any permutation σ on the coordinates of the vector $\boldsymbol{x} \in S^t$, $\lambda(\sigma(\boldsymbol{x})) = \lambda(\boldsymbol{x})$.

If $\lambda(\boldsymbol{x}) = \lambda(\boldsymbol{y})$ for every $\boldsymbol{x}, \boldsymbol{y} \in S^t$, then the array is called an *orthogonal array* of strength t, and denoted by $OA(N, k, s, t)$, where $N = \lambda s^t$. It is known that a balanced array is equivalent to a nested (r, λ)-design, shown in Kuriki and Fuji-Hara [8].

Let G be a $k \times n$ matrix over GF(q), a finite field of order q. Bose [2] showed that if any t rows of G are linearly independent, then the k-dimensional column vector space $\{Gx\,;\, x \in \mathrm{GF}(q)^n\}$ is an $OA(q^n, k, q, t)$ with $\lambda = q^{n-t}$.

As a generalization of Bose's method, Fuji-Hara and Miyamoto [3] proposed a collection A of k-dimensional column vectors. Let $f_1, f_2, \ldots, f_k$ be distinct multivariate functions with a domain W ($\subseteq \mathrm{GF}(q)^n$) in common. We define the collection A as

$$A = \left\{ \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_k(x) \end{pmatrix} \quad ; \quad x \in W \right\},$$

denoted by $A(f_1, f_2, \ldots, f_k; W)$ for convenience. We may regard it as an array with an arbitrary order of vectors. Using $A(f_1, f_2, \ldots, f_k; W)$, Fuji-Hara and Miyamoto [3] constructed an $OA(q^3, q^2, q, 2)$ and a $BA(q^2(q-1), q^2, q, 2)$ for any even prime power q. In this paper, for any odd prime power q, we construct a $BA(q^2(q-1), q^2, q, 2)$. Moreover we give a $BA(q^6 - q^3, q^2, q^2, 2)$ for any prime power q as an application of the results obtained here.

2 Generation of non-linear functions

In a finite projective geometry PG(n, q) of n dimension over a GF(q), the points are represented by $(n+1)$-tuples $x = (x_0, x_1, \ldots, x_n)'$, where $x_i \in \mathrm{GF}(q)$ for $i = 0, 1, \ldots, n$. The $(n+1)$-tuples $tx = (tx_0, tx_1, \ldots, tx_n)'$ is regarded as the same point as x for any non-zero $t \in \mathrm{GF}(q)$ and the null $(n+1)$-tuples $(0, 0, \ldots, 0)'$ is not a point of PG(n, q). A *projectivity* α : $\mathrm{PG}(n, q) \to \mathrm{PG}(n, q)$ is a bijection given by a matrix T: if $P' = P^\alpha$, then $tx' = Tx$, where x' and x are vector representations of points P' and P respectively, and a non-zero element $t \in \mathrm{GF}(q)$.

Now we use quadratic forms over GF(q) and projectivities in order to find a number of multivariate functions in Section 1. Let f be a quadratic form, that is, $f(x) = x'Qx = \sum q_{ij}x_ix_j$, where Q is a triangular matrix over GF(q). Then a variety $V(f) = \{x \in \mathrm{PG}(n, q)\,;\, f(x) = 0\}$ is called a *quadric*. In this paper, we consider non-degenerate quadrics in PG($3, q$), which are the following canonical forms:

Elliptic quadric : $V(dx_0^2 + x_0x_1 + x_1^2 + x_2x_3)$, where

$$q \text{ even} : d \in \{t \in \mathrm{GF}(2^h)\,;\, D(t) = t + t^2 + \cdots + t^{2^{h-1}} = 1\}$$
$$q \text{ odd} : d \in \{t \in \mathrm{GF}(q)\,;\, 1 - 4t \text{ is a non-square}\}$$

Hyperbolic quadric : $V(x_0x_1 + x_2x_3)$.

An elliptic quadric and a hyperbolic quadric consist of q^2+1 and $(q+1)^2$ points in PG$(3,q)$, respectively. If a plane of PG$(3,q)$ meets an elliptic quadric at one point, it is called a *tangent plane.* In a hyperbolic quadric, if a plane meets it in two lines, the plane and lines are called a *tangent plane* and *generators*, respectively.

From the definition of the balanced arrays, in order that $A(f_1, f_2, \ldots, f_k; \boldsymbol{W})$ is a balanced array, it is necessary that $|V(f_i) \cap V(f_j)|$ is independent of choice of i, j, $i \neq j$ in the domain $\boldsymbol{W}$. Therefore we use a projective group on PG$(3,q)$ to generate varieties systematically as many as possible. Let $V(f)$ be a quadric in PG$(3,q)$ and $\Gamma = \{\alpha_1 = 1, \alpha_2, \cdots, \alpha_g\}$ a projective group of order g on PG$(3,q)$. For any $\alpha_i \in \Gamma$, $V(f_i) = V(f)^{\alpha_i}$ is given by $f_i(x) = \boldsymbol{x}'\boldsymbol{T}_i'\boldsymbol{Q}\boldsymbol{T}_i\boldsymbol{x}$ for $i = 1, 2, \ldots, g$, where $f(x) = \boldsymbol{x}'\boldsymbol{Q}\boldsymbol{x}$ and $\boldsymbol{T}_i$ is a matrix representation of α_i. Then we can construct g quadrics:

$$V(f_1), V(f_2), \cdots, V(f_g), \text{such that } |V(f_i)| = |V(f_j)|, i \neq j.$$

In order to satisfy a condition $|V(f_i) \cap V(f_j)| = \mu$, $i \neq j$, we define a projective group on PG$(3,q)$ as follows:

Let $\alpha_{(\pi,V)}$ be a projectivity on PG$(3,q)$ which fixes a plane π pointwise and a point $V \in \pi$ linewise. There are q such projectivities on PG$(3,q)$ for given π, V. The set of q projectivities forms a projective group $\Gamma_{(\pi,V)}$ of order q. Moreover, we define $\Gamma_{(\pi,l)} = \bigcup_{V \in l} \Gamma_{(\pi,V)}$, where l is a line on π. It is also a projective group of order $q(q+1) - q = q^2$. Then we can generate q^2 quadratic functions $G = \{f_1, f_2, \ldots, f_{q^2}\}$ by using $\Gamma_{(\pi,l)}$. In next section we will find $G = \{f_1, f_2, \ldots, f_{q^2}\}$ is useful to construct a balanced array, where $V(f_i)$'s are elliptic or hyperbolic quadrics.

3 Constructions

The quadratic character χ of GF(q), q an odd prime power, is defined by

$$\chi(x) := \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \neq 0 \text{ is a square} \\ -1 & \text{otherwise.} \end{cases}$$

Then for any $a \neq 0$,

$$S := \sum_{x \in GF(q)} \chi(x)\chi(x-a) = -1. \tag{1}$$

We consider the set $N = \{(\chi(x), \chi(x-a))\ ;\ x \in \text{GF}(q)\}$ for an element $a \in \text{GF}(q)$. Let x, y, z, w be the numbers of elements of N with $(1,1)$, $(1,-1)$, $(-1,1)$, $(-1,-1)$, respectively. Then we have the following lemma.

Lemma 3.1 *When $q \equiv 1 \bmod 4$,*

$$\begin{array}{ll} x = y = z = \frac{q-1}{4}, \quad w = \frac{q-5}{4} & \text{if } a \text{ is a square} \\ x = \frac{q-5}{4}, \quad y = z = w = \frac{q-1}{4} & \text{if } a \text{ is a non-square} \end{array}$$

Proof. If a is a square, $\chi(-a) = 1$. Each of $(1, 0)$ and $(0, 1)$ appears exactly once in N. Hence we have the following system of equations:

$$\begin{cases} x + y + 1 = \frac{q-1}{2} \\ z + w = \frac{q-1}{2} \\ x + z + 1 = \frac{q-1}{2} \\ y + w = \frac{q-1}{2} \\ x + w + 1 = y + z. \end{cases}$$

The last of the above equations is from the equation (1). Its unique solution is $x = y = z = \frac{q-1}{4}$, $w = \frac{q-5}{4}$.

If a is a non-square, $\chi(-a) = -1$. Similarly we have the following system of equations:

$$\begin{cases} x + y = \frac{q-1}{2} \\ z + w + 1 = \frac{q-1}{2} \\ x + z = \frac{q-1}{2} \\ y + w + 1 = \frac{q-1}{2} \\ x + w + 1 = y + z. \end{cases}$$

Thus we have the unique solution $x = \frac{q-5}{4}$, $y = z = w = \frac{q-1}{4}$.

Lemma 3.2 *When $q \equiv 3 \bmod 4$,*

$$\begin{array}{ll} x = y = w = \frac{q-3}{4}, \quad z = \frac{q+1}{4} & \text{if } a \text{ is a square} \\ x = z = w = \frac{q-3}{4}, \quad y = \frac{q+1}{4} & \text{if } a \text{ is a non-square} \end{array}$$

Proof. This follows from the same manner as Lemma 3.1 and $n_{1j} = -n_{j1}$ for $q \equiv 3 \bmod 4$. ■

Now we consider the following three cases to construct arrays $A(f_1, f_2, \ldots, f_k; \boldsymbol{W})$.

Construction 1

$G_1 = \{f_1, f_2, \ldots, f_{q^2}\}$ is given by an elliptic quadric $V(f_1)$ in $\mathrm{PG}(3, q)$ and $\Gamma_{(\pi_0, l)}$, where l is an external line and π_0 is a tangent plane through l of $V(f_1)$.

$\boldsymbol{W}_1 = \pi_1 - l$, where π_1 is a non-fixed tangent plane of $V(f_1)$.

Construction 2

$G_1 = \{f_1, f_2, \ldots, f_{q^2}\}$ is given by an elliptic quadric $V(f_1)$ in $\mathrm{PG}(3, q)$ and $\Gamma_{(\pi_0, l)}$, where l is an external line and π_0 is a tangent plane through l of $V(f_1)$.

W_2 is a coset of $L(\pi_0)$ distinct from $L(\pi_0)$, where $L(\pi_0) = \{tx\ ;\ t \in \mathrm{GF}(q),\ x \in \pi_0\}$.

Construction 3

$G_2 = \{f_1, f_2, \ldots, f_{q^2}\}$ is given by a hyperbolic quadric $V(f_1)$ in $\mathrm{PG}(3,q)$ and $\Gamma_{(\pi_0,l)}$, where l is a generator and π_0 is a tangent plane through l of $V(f_1)$.

W_2 is a coset of $L(\pi_0)$ distinct from $L(\pi_0)$.

Without loss of generality, we may assume that f_1 of G_1 or G_2 is given by

(i) $f_1(x) \in G_1\ ;\ f_1(x) = dx_0^2 + x_0x_1 + x_1^2 + x_2x_3$ or

(ii) $f_1(x) \in G_2\ ;\ f_1(x) = x_0x_1 + x_2x_3$

and a projective group $\Gamma_{(\pi_0,l)}$ is represented by

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ a & b & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad {}^{\forall}a, b \in \mathrm{GF}(q),$$

where $l = \{(1,0,0,0)' \cup (t,1,0,0)'\ ;\ t \in \mathrm{GF}(q)\}$, $\pi_0 = \{(x_0,x_1,x_2,x_3)' \in \mathrm{PG}(3,q)\,;\, x_2 = 0\}$. Then the quadratic forms which are constructed by the above projective group is expressed by

(i) $f_i(x) \in G_1\ ;\ f_i(x) = dx_0^2 + x_0x_1 + (b+2ad)x_0x_2 + x_1^2 + (a+2b)x_1x_2 + (ab+b^2+a^2d)x_2^2 + x_2x_3,$

(ii) $f_i(x) \in G_2\ ;\ f_i(x) = x_0x_1 + bx_0x_2 + ax_1x_2 + abx_2^2 + x_2x_3,$

and W_1 and W_2 are given by

$W_1 = \{x = (x_0,x_1,x_2,x_3)' \in \mathrm{GF}(q)^4\ ;\ x_2 = 1,\ x_3 = 0\},$

$W_2 = \{x = (x_0,x_1,x_2,x_3)' \in \mathrm{GF}(q)^4\ ;\ x_2 = 1\}.$

We can say that the number of solutions to the system of equations for x

$$\begin{cases} f_i(x) &= \alpha \\ f_j(x) &= \beta \end{cases}$$

is equal to the number of solutions to

$$\begin{cases} f_1(x) &= \alpha \\ f_k(x) &= \beta \end{cases}$$

by using linear transformation ,where $k \in \{2,3,\ldots,q^2\}$ and $i,j = 1,2,\ldots,q^2$, $i \neq j$.

Here we show that the construction 1 gives a balanced array. We arrange the collection $A(f_1, f_2, \ldots, f_k; W)$ for the following:

$$A^* = \cup_{w \in \mathrm{GF}(q)^*} wA$$

where $\mathrm{GF}(q)^*$ is the non-zero elements of $\mathrm{GF}(q)$. Then A^* is described as $A^*(f_1, f_2, \ldots, f_k; W)$ over $\mathrm{GF}(q)^*$. To show $A^*(f_1, f_2, \ldots, f_k; W)$ is a balanced array, we may count the number of solutions to the system of equations

$$\begin{cases} f_1(x) &= dx_0^2 + x_0x_1 + x_1^2 + x_2x_3 = w\alpha \\ f_i(x) &= dx_0^2 + x_0x_1 + (b+2ad)x_0x_2 + x_1^2 \\ & \quad +(a+2b)x_1x_2 + (ab+b^2+a^2d)x_2^2 + x_2x_3 = w\beta \end{cases}$$

depending on values of the parameter $w \in \mathrm{GF}(q)^*$.

Theorem 3.1 *Let $W_2 = \pi_1 - l$ and $f_1, \ldots, f_k$ quadratic functions of G_1. Then $A^*(f_1, f_2, \ldots, f_k; W_1)$ is a $BA(q^2(q-1), q^2, q, 2)$, for odd prime power q with*

$$\mu(\alpha, \beta) = \begin{cases} 0 & \textit{if} \quad \alpha = \beta = 0 \\ 1 & \textit{if} \quad \textit{one of } \alpha \textit{ or } \beta \textit{ is } 0 \\ q & \textit{if} \quad \alpha = \beta \neq 0 \\ q+1 & \textit{if} \quad \alpha \neq \beta \neq 0 \end{cases} \tag{2}$$

Proof. It is sufficient to show the number of elements in

$$\cup_{w \in \mathrm{GF}(q)^*} \{x \in W_1 \; ; \; f_1^*(x) = 0 \text{ and } f_i^*(x) = 0\}$$

satisfies the above assertion (2) for any α, β, where

$$f_1^*(x) = dx_0^2 + x_0x_1 + x_1^2 - w\alpha x_2^2 + x_2x_3 = 0, \tag{3}$$

$$\begin{aligned} f_i^*(x) &= dx_0^2 + x_0x_1 + (b+2ad)x_0x_2 + x_1^2 + (a+2b)x_1x_2 \\ & \quad +(ab+b^2+a^2d - w\beta)x_2^2 + x_2x_3 = 0. \end{aligned} \tag{4}$$

By subtracting the equation (3) from the equation (4) and putting $x_2 = 1$, we have

$$(b+2ad)x_0 + (a+2b)x_1 + u + w(\alpha - \beta) = 0, \tag{5}$$

where $u = ab + b^2 + a^2d$. From the equation (3) and (5), we obtain the quadratic equation for x_0

$$\begin{aligned} & u(1-4d)x_0^2 + a(1-4d)(u + w(\alpha-\beta))x_0 \\ & \quad + w\alpha(a+2b)^2 - (u + w(\alpha - \beta))^2 = 0. \end{aligned} \tag{6}$$

The discriminant Δ of (6) is

$$\Delta = (1-4d)(a+2b)^2((u+w(\alpha-\beta))^2 - 4uw\alpha).$$

In order to have a solution to (6), Δ must be zero or a square element of GF(q). That is $\Delta' = (u+w(\alpha-\beta))^2 - 4uw\alpha$ should be zero or a non-square. We consider the number of solutions for x_0 to the equation (6) depending on values of the parameter w.

Case 1, $\alpha = \beta = 0$
From $\Delta' = u^2$ and $u \neq 0$, the equation (6) has no solution.

Case 2, $\alpha = 0$ or $\beta = 0$
If $\alpha = 0$, then $\Delta' = (u - w\beta)^2$. So the equation (6) has one solution when $w = u\beta^{-1}$. Similarly, if $\beta = 0$, the equation (6) has one solution when $w = u\alpha^{-1}$.

Case 3, $\alpha = \beta \neq 0$
There are two solutions to the equation (6) when the w is one of $\frac{q-1}{2}$ different values such that $\Delta' = u^2 - 4uw\alpha$ is a non-square. Moreover there is one solution when $w = u(4\alpha)^{-1}$ such that Δ' is zero. Hence there exist totally q solutions in the domain $\boldsymbol{W}_1$.

Case 4, $\alpha \neq \beta \neq 0$
When we put $\alpha = 1$, $\Delta' = (u+w(1-\beta))^2 - 4uw$. Consider a solution to $(1-\beta)^2w^2 - 2u(1+\beta)w + u^2 - \Delta' = 0$ for w. Then the discriminant $\Delta'' = (1-\beta)^2\Delta' + 4\beta u^2$ must be zero or a square element of GF(q). If $\Delta' = 0$ and β is a square, then $\Delta'' = 4\beta u^2$ becomes a square. So there are two solutions for w.

Next consider the case of Δ' a non-square. Let

$$N_1 = |\{\Delta' \in \mathrm{GF}(q)^*; \chi(\Delta') = -1 \text{ and } \chi((1-\beta)^2\Delta' + 4\beta u^2) = 0\}|,$$

$$N_2 = |\{\Delta' \in \mathrm{GF}(q)^*; \chi(\Delta') = -1 \text{ and } \chi((1-\beta)^2\Delta' + 4\beta u^2) = 1\}|.$$

In case of $q \equiv 1 \pmod 4$, $N_1 = 1$ if β is a non-square and $N_1 = 0$ if β is a square. From Lemma 3.1 and $\chi((1-\beta)^2\Delta') = \chi(\Delta')$ for all $\Delta' \in \mathrm{GF}(q)$, $N_2 = \frac{q-1}{4}$. When w is one of $\frac{q-1}{4} \times 2 + 1 = \frac{q+1}{2}$ different values and β is a non-square, the equation (6) has two solutions. When w is one of $\frac{q-1}{4} \times 2$ different values and β is a square, the equation (6) has also two solutions. Hence there exist $q+1$ solutions in the domain $\boldsymbol{W}_1$ when β is a non-zero element of GF(q).

In case of $q \equiv 3 \pmod 4$, $N_1 = 0$ if β is a non-square and $N_1 = 1$ if β is a square. From Lemma 3.2, $N_2 = \frac{q+1}{4}$ if β is a non-square and $N_2 = \frac{q-3}{4}$ if β is a square. When w is one of $\frac{q+1}{4} \times 2 = \frac{q+1}{2}$ different values and β is a non-square, the equation (6) has two solutions. When w is one of $\frac{q-3}{4} \times 2 + 1 = \frac{q-1}{2}$ different values and β is a square, the equation (6) has two solutions. Thus in both cases , β is a square or a non-square , we have totally $q+1$ solutions in the domain W_1.

We complete the proof for any $\alpha, \beta \in \mathrm{GF}(q)$. ■

Next we consider the construction 2 and 3. We will find that these constructions give orthogonal arrays and balanced arrays. The following result is from [9] which is a generalized case of the theorem of Bézout:

Result 3.1 *If the intersection of $V(f_1)$ and $V(f_2)$ is a curve C, then the degree of C is $n_1 n_2$, where n_1 and n_2 are the degree of f_1 and f_2, respectively.*

This is useful to show next two lemmas. The parameters of the $OA(q^3, q^2, q, 2)$ in Lemma 3.3 and 3.4 are not new. The orthogonal arrays are not a linear subspace themselves, although they may be cosets of a linear subspace.

Lemma 3.3 *Let W_2 be a coset of $L(\pi_0)$ distinct from $L(\pi_0)$ and $f_1, \ldots, f_k$ quadratic functions of G_1. Then $A(f_1, f_2, \ldots, f_k; W_2)$ is an $OA(q^3, q^2, q, 2)$, for any prime power q with $\lambda = q$.*

Proof. We will show that the number of solutions to the system of equations for x

$$\left\{ \begin{array}{rcl} f_1(x) & = & dx_0^2 + x_0x_1 + x_1^2 + x_2x_3 = \alpha \\ f_i(x) & = & dx_0^2 + x_0x_1 + (b+2ad)x_0x_2 + x_1^2 \\ & & +(a+2b)x_1x_2 + (ab+b^2+a^2d)x_2^2 + x_2x_3 = \beta \end{array} \right. \tag{7}$$

is q for any $\alpha, \beta \in \mathrm{GF}(q)$. Since we put the domain $W_2 = \{x = (x_0, x_1, x_2, x_3)' \in \mathrm{GF}(q)^4 \,;\, x_2 = 1\}$, it is the same as the number of solutions to the system of equations for x

$$\left\{ \begin{array}{rcl} f_1^*(x) & = & dx_0^2 + x_0x_1 + x_1^2 - \alpha x_2^2 + x_2x_3 = 0 \\ f_i^*(x) & = & dx_0^2 + x_0x_1 + (b+2ad)x_0x_2 + x_1^2 \\ & & +(a+2b)x_1x_2 + (ab+b^2+a^2d-\beta)x_2^2 + x_2x_3 = 0. \end{array} \right.$$

Hence it is sufficient to consider the intersection of elliptic quadric $V(f_1^*)$ and $V(f_i^*)$ in $\mathrm{PG}(3,q)$. Extend the space $\mathrm{PG}(3,q)$ to $\mathrm{PG}(3,q^2)$, then $V(f_1^*)$ becomes a hyperbolic quadric in $\mathrm{PG}(3,q^2)$. In the quadratic extension $\mathrm{PG}(3,q^2)$ of $\mathrm{PG}(3,q)$, the tangent plane π_0 of the hyperbolic quadric $V(f_1^*)$ intersects $V(f_1^*)$ in two lines l_1 and l_2. Since π_0 is fixed by $\Gamma_{(\pi_0,l)}$ pointwise, l_1 and l_2 lie in $V(f_i^*)$. So $V(f_1^*)$ and $V(f_i^*)$ already have two lines l_1 and l_2 of $\mathrm{PG}(3,q^2)$ in common.

From Result 3.1, $V(f_1^*)$ and $V(f_i^*)$ intersect in a curve of degree 4. Since the curve of degree 4 already contains two lines l_1 and l_2, the remaining part of the intersection in $PG(3,q^2)$ is a curve of degree 2. The curve of degree 2 is the union of two lines or a conic in a plane. But each of $V(f_1^*)$ and $V(f_i^*)$ contains no line of $PG(3,q)$. Therefore, in $PG(3,q)$, $V(f_1^*)$ meets $V(f_i^*)$ in a conic which consists of q points and the fixed point $l_1 \cap l_2$. Thus the number of solutions to the system of equations (7) is q in W_2 for any $\alpha, \beta \in GF(q)$. ■

Lemma 3.4 *Let W_2 be a coset of $L(\pi_0)$ distinct from $L(\pi_0)$ and $f_1, \dots, f_k$ quadratic functions of G_2. Then $A(f_1, f_2, \dots, f_k; W_2)$ is an $OA(q^3, q^2, q, 2)$, for any prime power q with $\lambda = q$.*

Proof. Similar to Lemma 3.3, we will show that the hyperbolic quadrics $V(f_1^*)$ and $V(f_i^*)$ have $3q+1$ points of $PG(3,q)$ in common , where

$$\begin{aligned} f_1^*(x) &= x_0x_1 - \alpha x_2^2 + x_2x_3 = 0, \\ f_i^*(x) &= x_0x_1 + bx_0x_2 + ax_1x_2 + (ab-\beta)x_2^2 + x_2x_3 = 0. \end{aligned}$$

$V(f_1^*)$ and $V(f_i^*)$ are hyperbolic quadrics also in the quadratic extension $PG(3,q^2)$. By using the same argument of the previous proof, the intersections of $V(f_1^*)$ and $V(f_i^*)$ consist of two lines l_1, l_2 on π_0 and a curve of degree 2 in $PG(3,q^2)$. If the curve is the union of two lines, then one of them is the line l_1 or l_2. Hence in both cases, $V(f_1^*)$ meets $V(f_i^*)$ in $3q+1$ points of $PG(3,q)$. Therefore the number of solutions in W_2 to the system of equations $\begin{cases} f_1(x) = \alpha \\ f_i(x) = \beta \end{cases}$ for x is q for any $\alpha, \beta \in GF(q)$. ■

Moreover, we consider a domain W_3 on $PG(3,q^2)$. Let $\bar{\pi}_0 = \{x \in PG(3,q^2)\,; x \in \pi_0\}$ and $\bar{L}(\bar{\pi}_0) = \{tx\,;\, t \in GF(q^2),\ x \in \bar{\pi}_0\}$. Then we define W_3 as a coset of $\bar{L}(\bar{\pi}_0)$ distinct from $\bar{L}(\bar{\pi}_0)$. Next two theorems are immediate from Lemma 3.3 and 3.4.

Theorem 3.2 *Let W_2 be a coset of $L(\pi_0)$ distinct from $L(\pi_0)$, let W_3 be a coset of $\bar{L}(\bar{\pi}_0)$ distinct from $\bar{L}(\bar{\pi}_0)$ and $f_1, \dots, f_k$ quadratic functions of G_1. Then $A(f_1, f_2, \dots, f_k; W_3 - W_2)$ is a $BA(q^6 - q^3, q^2, q^2, 2)$, for any prime power q with*

$$\mu(\alpha,\beta) = \begin{cases} q^2 - q & \text{if} \quad \alpha,\beta \in GF(q) \\ q^2 & \text{if} \quad \text{otherwise} \end{cases}$$

Proof. From Lemma 3.3, the number of solutions to the system of equations (7) in W_3 is q^2 for any $\alpha, \beta \in GF(q^2)$ and the number of solutions to the system of equations (7) in W_2 is q for any $\alpha, \beta \in GF(q)$. Therefore the number of solutions to the system equations (7) in $W_3 - W_2$ is $q^2 - q$ for any $\alpha, \beta \in \mathrm{GF}(q)$. ■

Theorem 3.3 *Let W_2 be a coset of $L(\pi_0)$ distinct from $L(\pi_0)$, let W_3 be a coset of $\bar{L}(\bar{\pi}_0)$ distinct from $\bar{L}(\bar{\pi}_0)$ and $f_1, \ldots, f_k$ quadratic functions of G_2. Then $A(f_1, f_2, \ldots, f_k; W_3 - W_2)$ is a $BA(q^6 - q^3, q^2, q^2, 2)$, for any prime power q with*

$$\mu(\alpha, \beta) = \begin{cases} q^2 - q & \text{if} \quad \alpha, \beta \in GF(q) \\ q^2 & \text{if} \quad \text{otherwise} \end{cases}$$

Proof. Similar to Theorem 3.2. ■

References

[1] Th. Beth, D. Jungnickel and H. Lenz (1985), *Design Theory*, Wissenschaftsverlag.

[2] R.C. Bose, *Mathematical theory of the symmetrical factorial design*, Sankhya 8 (1947),107-166.

[3] R. Fuji-Hara and N. Miyamoto, *Balanced Arrays from Quadratic Functions*, submitted to J.S.P.I.

[4] J.W.P. Hirschfeld (1979), *Projective Geometries over Finite Field*, Oxford University Press, New York.

[5] J.W.P. Hirschfeld (1985), *Finite Projective Spaces of Three Dimensions*, Oxford University Press, New York.

[6] D.R. Hughes and Piper (1973), *Projective Planes*, Springer-Verlag, New York.

[7] S. Kuriki (Private communication).

[8] S. Kuriki and R. Fuji-Hara *Balanced Arrays of Strength Two and Nested (r, λ)-Designs*, J.C.D. Vol.2 No.6 (1994), 407-414.

[9] J.G. Semple and L. Roth (1986), *Introduction to Algebraic Geometry*, Oxford University Press, Oxford.