No. 757

Balanced Arrays from Quadratic Functions

by

Ryoh Fuji-Hara and Nobuko Miyamoto

October 1997

Balanced Arrays from Quadratic Functions

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

Management Science and Engineering,
Institute of Socio-Economic Planning, University of Tsukuba,
Tsukuba, Ibaraki, Japan 305

Abstract

There is a famous construction of orthogonal arrays by R.C. Bose (1947). The construction uses linear transformations over a finite field. We generalize this to use non-linear transformation instead of linear and a subset of vector space as their domains.
We show here constructions of orthogonal and balanced arrays which are generated by a set of quadratic function.

1 Introduction

Let S be a set $\{0, 1, \ldots, s-1\}$ of s symbols and let S^t the set of all t-dimensional column vectors over S. A balanced array of strength t, denoted by $BA_\lambda(n, k, s, t)$ 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 A_0.

(ii) for any permutation σ on any t-column 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 $n = \lambda s^2$.

A balanced array was first introduced by Chakravarti [2] in connection with some class of statistical designs. Since then, many interesting result on the balanced arrays are shown in Srivastava [6] and Rafter and Seidan

[5]. As a special case of balanced arrays, Horton [3] defined an incomplete orthogonal array, denoted by $IOA(n, k, s, h, t)$, as follows.

Let H be a h-subset of S and H^t the set of all t-dimensional column vectors over H.

(iii) in any t-rowed subarray $\boldsymbol{A}_0$ of $\boldsymbol{A}$, every $\boldsymbol{x} \in S^t \setminus H^t$ appears $\lambda(\boldsymbol{x})$ times in A_0.

In order to construct such balanced arrays, we introduce in Section 2 a construction of orthogonal array which are proposed by Bose. And we generalize this method by restricting a domain and using multivariate functions. In Section 3, we generate quadratic functions from a eliiptic quadric and a collineation group. Finally we give new constructions of orthogonal and balanced arrays of strength 2.

2 Genalization of Bose's construction

Bose [1] proposed a useful construction of orthogonal arrys as follows.

The construction of Bose

Let $\boldsymbol{G}$ be a $k \times m$ matrix over GF(q). If any t rows of $\boldsymbol{G}$ are independent, a set of k dimensional vector which is generated by $\boldsymbol{G}$;

$$\{\boldsymbol{G}\boldsymbol{x}' \,;\, \boldsymbol{x} \in \mathrm{GF}(q)^m\}$$

where $\boldsymbol{x}'$ is a transpose of $\boldsymbol{x}$ is an $OA(q^m, k, q, t)$ with $\lambda = q^{m-t}$.

We consider a linear combination $\boldsymbol{g}\boldsymbol{x}'$ as a linear function $f(\boldsymbol{x}) = g_1x_1 + g_2x_2 + \ldots + g_mx_m$ where $\boldsymbol{g} = (g_1, g_2, \ldots, g_m)$, $\boldsymbol{x} = (x_1, x_2, \ldots, x_m)$. Then we interpret the method of Bose as follows.

For all $\boldsymbol{x} \in \mathrm{GF}(q)^m$,

$$\boldsymbol{G}\boldsymbol{x}' = \begin{pmatrix} f_1(\boldsymbol{x}) = g_{11}x_1 + g_{12}x_2 + \ldots + g_{1m}x_m \\ f_2(\boldsymbol{x}) = g_{21}x_1 + g_{22}x_2 + \ldots + g_{2m}x_m \\ \vdots \\ f_k(\boldsymbol{x}) = g_{k1}x_1 + g_{k2}x_2 + \ldots + g_{km}x_m \end{pmatrix}$$

where g_{ij} is the (i,j)-th element of a matrix $\boldsymbol{G}$.

Moreover we generalize this method and define a set A satisfying the following conditions:

$$A = \left\{ \begin{pmatrix} f_1(x_1, x_2, \ldots, x_m) \\ f_2(x_1, x_2, \ldots, x_m) \\ \cdot \\ \cdot \\ \cdot \\ f_k(x_1, x_2, \ldots, x_m) \end{pmatrix} \; ; \; (x_1, x_2, \ldots, x_m) \in \boldsymbol{W} \right\}$$

(1) $\boldsymbol{W}$ is a domain of f_i which is a subset of $\mathrm{GF}(q)^m$,

(2) $f_1, f_2, \cdots, f_k$ are multivariate functions.

The set A is denoted by $A(f_1, f_2, \ldots, f_k; \boldsymbol{W})$ for convenience. We first introduce some constructions by restricting a domain $\boldsymbol{W}$ and letting f_i be linear functions.

Example Let $\boldsymbol{W}$ be $\mathrm{GF}(q^m)^t - \mathrm{GF}(q)^t$ and $f_1, f_2, \cdots, f_k$ be linear functions over $\mathrm{GF}(q)$ where any t functions of them are independent. Then $A(f_1, f_2, \ldots, f_k; \boldsymbol{W})$ is an $IOA(q^{mt} - q^t, k, q^m, q, t)$ with $\lambda = 1$.

Proof.

We must show $A(f_1, f_2, \ldots, f_k; \boldsymbol{W})$ contains every t-column vector from $\mathrm{GF}(q^m)^t - \mathrm{GF}(q)^t$ precisely one. First, we consider a domain $\boldsymbol{W}$ as $\mathrm{GF}(q^m)^t$. Let $(a_1, a_2, \ldots, a_t)$ be any t-vector from $\mathrm{GF}(q^m)^t$. Since $f_1, f_2, \ldots, f_t$ are linearly independent, the number of solutions for $\boldsymbol{x}$ which satisfy

$$\begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_t \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_t \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_t \end{pmatrix}$$

is one for every $(a_1, a_2, \ldots, a_t) \in \mathrm{GF}(q^m)^t$. Secondly, we consider a domain $\boldsymbol{W}'$ as $\mathrm{GF}(q)^t$. Let $(a_1, a_2, \ldots, a_t)$ be any t-vector from $\mathrm{GF}(q)^t$. The number of solutions for $\boldsymbol{x}$ which satisfy above equation is also one. We restrict a domain $\boldsymbol{x}$ to $\mathrm{GF}(q^m)^t - GF(q)^t = \boldsymbol{W} - \boldsymbol{W}'$. Then for each $(a_1, a_2, \ldots, a_t) \in \mathrm{GF}(q^m)^t - GF(q)^t$, there is exactly one solution for $\boldsymbol{x}$. □

Example Let $\boldsymbol{W}$ be a hyperplane $\mathcal{H}$ of $\mathrm{GF}(q)^m$ and $f_1, f_2, \cdots, f_k$ be linear functions and null space of any two f_i, f_j $(i \neq j)$ is not parallel to $\mathcal{H}$. Then $A(f_1, f_2, \ldots, f_k; \boldsymbol{W})$ is an $OA(q^{m-1}, k, q, 2)$ with $\lambda = q^{m-3}$.

Proof.

A hyperplane $\mathcal{H}$ is an $m-1$ dimensional sub-space over $\mathrm{GF}(q)$ and it contains q^{m-1} points. The sub-space which is generated by $f_i(\boldsymbol{x})$, $\boldsymbol{x} \in \mathcal{H}$, is also an $m-1$ dimensional sub-space $\mathcal{H}_i$. The intersection of $\mathcal{H}$ and $\mathcal{H}_i$ is an $m-2$ dimensional sub-space. Hence the set $\boldsymbol{x}$ satisfying

$$\begin{pmatrix} f_i(\boldsymbol{x}) \\ f_j(\boldsymbol{x}) \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$$

for any $a, b \in \mathrm{GF}(q)$ is an $m-3$ dimensional sub-space over $\mathrm{GF}(q)$. So the frequencies of (a, b) is q^{m-3}. □

3 Generation of quadratic functions

When $A(f_1, f_2, \ldots, f_k; \boldsymbol{W})$ is a balanced array, $\boldsymbol{x} \in S^2$ appears $\lambda(\boldsymbol{x})$ times in any 2-rowed subarray of $A(f_1, f_2, \ldots, f_k; \boldsymbol{W})$. Consider the set of all $\boldsymbol{x} \in \boldsymbol{W}$ such that $f_i(\boldsymbol{x}) = 0$. Such a set is called variety in $\boldsymbol{W}$ and denoted by $V(f_i)$. Hence we have a necessary condition for balanced array using varieties. The following theorem is trivial since $|V(f_i) \cap V(f_j)|$ is eqaul to the frequencies of $(0, 0)$ in any i-th, j-th rows of $A(f_1, f_2, \ldots, f_k; \boldsymbol{W})$.

Theorem 3.1 *Suppose the cardinality of $V(f_i)$ in $\boldsymbol{W}$ is the same for i. If $A(f_1, f_2, \ldots, f_k; \boldsymbol{W})$ is a balanced array, then $|V(f_i) \cap V(f_j)|$ in $\boldsymbol{W}$ is independent of choice of i, j.*

Now we use quadratic forms of quadrics and automorphism group in order to find many multivariate functions f_i which satisfy Theorem 3.1 .

A quadric $\mathcal{F} = V(F)$ in $\mathrm{PG}(3, q)$ is given by a quadratic form $F = \sum a_{ij} x_i x_j$. In $\mathrm{PG}(3, q)$ with q even, an elliptic quadric has the following canonical form:

$$F = dx_0^2 + x_0 x_1 + x_2 x_3,$$

$^{\forall}d \in C_1 = \{t \in \mathrm{GF}(2^h)\, ;\, D(t) = t + t^2 + \cdots + t^{2^{h-1}} = 1\}$.

If S and S' are two spaces of $\mathrm{PG}(3,q)$, then a collineation $\alpha : S \rightarrow S'$ is a bijection which preserves incidence relation. A collineation α is written by $M(\boldsymbol{T})$ where $\boldsymbol{T}$ is a corresponding matrix of α.

Consider a collineation α on $\mathrm{PG}(3,q)$ which fixes a plane π pointwise and a point V on π linewise. Let Γ be any collineation group of $\mathrm{PG}(3,q)$ and l a line on π. Then we define $\Gamma_{(\pi,l)}$ as the union of such a collineation of Γ for any V on l. Note that $\Gamma_{(\pi,l)}$ forms a group with order q^2 and for any $\alpha, \beta \in \Gamma_{(\pi,l)}$, there exists $\gamma \in \Gamma_{(\pi,l)}$ such that $\alpha = \beta\gamma$.

Let $\mathcal{E} = V(F_1)$ with $F_1 = \boldsymbol{x}\boldsymbol{A}\boldsymbol{x}'$ be an elliptic quadric in $\mathrm{PG}(3,q)$ with $q > 2$ even, and l a external line to $\mathcal{E}$. There are two tangent planes π_0 and π_1 of $\mathcal{E}$ through l. Consider a group $\Gamma_{(\pi_0,l)}$ which fixes a tangent plane π_0. After this we use above notations in this meanings.

For any $\alpha = M(\boldsymbol{T}_i) \in \Gamma_{(\pi_0,l)}$, $\mathcal{E}^\alpha = V(F_i)$ is given by $F_i = \boldsymbol{x}\boldsymbol{T}_i\boldsymbol{A}\boldsymbol{T}_i'\boldsymbol{x}'$ $(i = 1, 2 \ldots, q^2)$. Then we define the set of quadratic functions G as follows.

$$G = \{F_1, F_2, \ldots, F_{q^2}\}$$

where $F_1, F_2, \ldots, F_{q^2}$ are quadratic forms of $\{\mathcal{E}^\alpha ; \alpha \in \Gamma_{(\pi_0,l)}\}$ respectively. It will be shown in the later chapter the set G satisfies Theorem 3.1 .

4 Constructions of balanced arrays

Preparatory to constructions, we give the discriminant of quadratic equation for q even. To solve, over $\mathrm{GF}(q)$ with $q = 2^h$, the quadratic equation

$$ax^2 + bx + c = 0, \quad a \neq 0 \tag{1}$$

the two cases are considered. If $b = 0$, then the equation (1) has one solution $x = \sqrt{\frac{c}{a}}$.

If $b \neq 0$, let $\delta = \frac{ac}{b^2}$ and $D(t) = t + t^2 + \cdots + t^{2^{h-1}}$.

If $D(\delta) = 0$, then the equation(1) has two solutions. If $D(\delta) = 1$, then the equation(1) has no solutions. Moreover we have the following well-known results.

Result 4.1 *Let $C_0 = \{t \in GF(q)\, ;\, D(t) = 0\}$ and $C_1 = \{t \in GF(q)\, ;\, D(t) = 1\}$ for $q = 2^h$.*

(i) $0 \in C_0$,

(ii) $t \in C_i \Rightarrow t^\sigma \in C_i$ *for any automorphism* σ *of* $GF(q)$,

(iii) $s \in C_i, t \in C_j \Rightarrow s+t \in C_0$ *if* $i=j$, $s+t \in C_1$ *if* $i \neq j$,

(iv) $|C_0| = |C_1| = \frac{q}{2}$.

Lemma 4.1 *Let* $t = k/(ax+bx^{-1})^2$ $(k,a,b \neq 0)$ *for* $x \in GF(q)$ *with* $q = 2^h$, $h \geq 2$. *Then* $|\{t \in GF(q)\,;\, t \in C_1\}|$ *is zero if* $k = ab$ *and* $\frac{q}{4}$ *if* $k \neq ab$.

Proof. Suppose $t \in C_1$. An equation $ta^2X^2 + kX + tb^2 = 0$ where $X = x^2$ must have two solutions. Let $\delta = t^2a^2b^2/k^2$. Since $\delta \in C_0$, we have a condition $\frac{ab}{k}t \in C_0$. Consider the following two cases:
Case 1
If $k \neq ab$, then $t \in C_0$ which contradicts assumption. Hence there is no t such that $t \in C_1$.
Case 2
If $k \neq ab$, then we consider the intersection of $\{t \in \mathrm{GF}(q)\,;\, t \in C_1\}$ and $\{t \in \mathrm{GF}(q)\,;\, \frac{ab}{k}t \in C_0\}$. Since $\mathrm{GF}(2^h) \cong \mathrm{GF}(2)^h$, let $S = \{\xi \in \mathrm{GF}(2)^h\,;\, \xi \in C_0\}$. S is a subspace of $\mathrm{GF}(2)^h$ and $|S| = \frac{q}{2}$. Then S is regarded as a hyperplane of $\mathrm{GF}(2)^h$. That is, the incidence matrix of elements of $\mathrm{GF}(2)^h \setminus \{0\}$ and the hyperplanes is a Hadarmard design $S_\lambda(2, 2^{h-1}-1, 2^h-1)$ with $\lambda = 2^{h-2}$. Hence $|\{t \in \mathrm{GF}(q)\,;\, t \in C_1\} \cap \{t \in \mathrm{GF}(q)\,;\, \frac{ab}{k}t \in C_0\}| = 2^{h-2} = \frac{q}{4}$. □

Lemma 4.2 *If any collineation of* $\Gamma_{(\pi,l)}$ *fixes no point in a domain* $\boldsymbol{W}$, *then for given* $a, b \in GF(q)$, *the number of solutions for* $\boldsymbol{x}$ *in the system of equations*

$$\begin{cases} F_i(\boldsymbol{x}) &= a \\ F_j(\boldsymbol{x}) &= b \end{cases}$$

equals to the number of solutions in

$$\begin{cases} F_1(\boldsymbol{x}) &= a \\ F_k(\boldsymbol{x}) &= b \end{cases}$$

where $F_1, F_i, F_j, F_k \in G$.

Proof. Let $F_i(\boldsymbol{x}) = \boldsymbol{x}\boldsymbol{T}_i\boldsymbol{A}\boldsymbol{T}_i'\boldsymbol{x}'$ and $F_j(\boldsymbol{x}) = \boldsymbol{x}\boldsymbol{T}_j\boldsymbol{A}\boldsymbol{T}_j'\boldsymbol{x}'$ where $\boldsymbol{T}_i, \boldsymbol{T}_j \in \Gamma_{(\pi,l)}$. Since there are no fixed points in $\boldsymbol{W}$, $\boldsymbol{x}\boldsymbol{T}_i$ runs over $\boldsymbol{W}$. Let $\boldsymbol{x}\boldsymbol{T}_i = y$. Hence we have the following two equations:

$$|\{\boldsymbol{x} \in \boldsymbol{W} \,;\, \boldsymbol{x}\boldsymbol{T}_i\boldsymbol{A}\boldsymbol{T}_i'\boldsymbol{x}' = a\}| = |\{\boldsymbol{y} \in \boldsymbol{W} \,;\, \boldsymbol{y}\boldsymbol{A}\boldsymbol{y}' = a\}|,$$

$$|\{\boldsymbol{x} \in \boldsymbol{W} \,;\, \boldsymbol{x}\boldsymbol{T}_j\boldsymbol{A}\boldsymbol{T}_j'\boldsymbol{x}' = b\}| = |\{\boldsymbol{y} \in \boldsymbol{W} \,;\, \boldsymbol{y}\boldsymbol{T}_i^{-1}\boldsymbol{T}_j\boldsymbol{A}\boldsymbol{T}_j'\boldsymbol{T}_i^{-1'}\boldsymbol{y}' = b\}|.$$

Therefore, for $F_k(\boldsymbol{x}) = \boldsymbol{x}\boldsymbol{T}_i^{-1}\boldsymbol{T}_j\boldsymbol{A}\boldsymbol{T}_j'\boldsymbol{T}_i^{-1'}\boldsymbol{x}'$,

$$|\{\boldsymbol{x} \in \boldsymbol{W} \,;\, F_i(\boldsymbol{x}) = a, F_j(\boldsymbol{x}) = b\}| = |\{\boldsymbol{x} \in \boldsymbol{W} \,;\, F_1(\boldsymbol{x}) = a, F_k(\boldsymbol{x}) = b\}|$$

is established. □

Next we consider a domain $\boldsymbol{W}$ of functions of G. Any point of PG$(3,q)$ is denoted by an 4-dimensional coordinate $\boldsymbol{x} = (x_0, x_1, x_2, x_3)$. Let $S = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$. We define $L(S)$ as follows:

$$L(S) = \{t\boldsymbol{x}_i \,;\, t \in \mathrm{GF}(q),\ \boldsymbol{x}_i \in S\}.$$

Then we restrict their domain to the following two cases by using $L(S)$.

(i) $\boldsymbol{W}_1$ is a coset of $L(\pi_0)$ distinct from $L(\pi_0)$
where π_0 is a fixed tangent plane of $\mathcal{E}$.

(ii) $\boldsymbol{W}_2 = L(\pi_1 \setminus l)$
where π_1 is a non-fixed tangent plane and l is a external line of $\mathcal{E}$.

Without loss of generality, we may assume that $\mathcal{E} = V(F_1)$ where

$$F_1 = x_0x_2 + x_1^2 + wx_1x_3 + x_2^2 + x_3^2,\ (\frac{1}{w} \in C_1)$$

and

$$l = \{(0,1,0,t) \cup (0,0,0,1); t \in \mathrm{GF}(q)\}.$$

Since two tangent planes of $\mathcal{E}$ are denoted by

$$\pi_0 = \{(x_0,x_1,x_2,x_3) \in \mathrm{PG}(3,q); x_2 = 0\}, \pi_1 = \{(x_0,x_1,x_2,x_3) \in \mathrm{PG}(3,q); x_0 = x_2\},$$

suppose that π_0 is fixed and π_1 is not fixed by $\Gamma_{(\pi_0,l)}$.
Then any collineation $\alpha = M(\boldsymbol{T})$ of $\Gamma_{(\pi_0,l)}$ is expressed by

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

and $\boldsymbol{W}_1$ and $\boldsymbol{W}_2$ are given by

$$\boldsymbol{W}_1 = \{\boldsymbol{x} = (x_0, x_1, x_2, x_3) \in \mathrm{GF}(q)^4 \, ; \, x_2 = 1\},$$

$$\boldsymbol{W}_2 = \{\boldsymbol{x} = (x_0, x_1, x_2, x_3) \in \mathrm{GF}(q)^4 \, ; \, x_0 = x_2, \, x_0 \neq 0\}.$$

By using a matrix $\boldsymbol{T}$ and a quadratic form F_1, we have $\mathcal{E}^{\alpha} = V(F_2)$ where

$$F_2 = x_0x_2 + x_1^2 + cwx_1x_2 + wx_1x_3 + (1 + a^2 + c^2 + acw)x_2^2 + awx_2x_3 + x_3^2.$$

Theorem 4.3 *Suppose that $\boldsymbol{W}_1$ is a coset of $L(\pi_0)$ distinct from $L(\pi_0)$ and $f_1, \ldots, f_k$ be quadraric functions of G respectively. Then $A(f_1, f_2, \ldots, f_k; \boldsymbol{W}_1)$ is an $OA(q^3, q^2, q, 2)$, $q = 2^h$, $h \geq 2$, with $\lambda = q$.*

Proof.
We will show that the number of solutions for $\boldsymbol{x}$ in the system equations

$$\begin{cases} F_1 = x_0x_2 + x_1^2 + wx_1x_3 + x_2^2 + x_3^2 = \alpha & (2) \\ F_2 = x_0x_2 + x_1^2 + cwx_1x_2 + wx_1x_3 & \\ \qquad +(1 + a^2 + c^2 + acw)x_2^2 + awx_2x_3 + x_3^2 = \beta & (3) \end{cases}$$

is q for any $\alpha, \beta \in \mathrm{GF}(q)$. It suffices to show $A(f_1, f_2, \ldots, f_k; \boldsymbol{W}_1)$ is an $OA(q^3, q^2, q, 2)$ from Lemma 4.2 .
By adding the equation(2) to the equation(3),

$$x_2\{cwx_1 + (a^2 + c^2 + acw)x_2 + awx_3\} = \alpha + \beta. \qquad (4)$$

Since $\boldsymbol{W}_1$ is restricted to a coset of $A_f(\pi_0)$, we may put $x_2 = 1$. Then we have a condition $cwx_1 + ux_2 + awx_3 = \alpha + \beta$ where $u = a^2 + c^2 + acw \neq 0$. We consider the following two cases:

Case 1
Let $a \neq 0$. By substituting $x_3 = a^{-1}cx_1 + (u+\alpha+\beta)(aw)^{-1}$ into the equation(2), we have a quadratic equation as follows.

$$ux_1^2 + (\alpha+\beta+u)ax_1 + (\alpha+\beta+u)^2w^{-2} + (\alpha+1+x_0)a^2 = 0 \qquad (5)$$

If $\alpha+\beta = u$, then the equation(5) has one solution for each $x_0 \in \mathrm{GF}(q)$. Secondary, if $\alpha+\beta \neq u$, then the equation(5) has two solutions on condition $D(\delta) = 0$ where $\delta = u/(a^2w^2) + u(\alpha+1+x_0)/(\alpha+\beta+u)$. From Result 4.1 , we have

$$D(\frac{u}{a^2w^2}) = D(\frac{1}{w^2}) + D(\frac{c}{aw} + \frac{c}{aw}^2) = 1 + 0 = 1.$$

And there are $\frac{q}{2}$ solutions x_0 such that $D(u(\alpha+1+x_0)/(\alpha+\beta+u)) = 1$. Hence there are q solutions in domain $\boldsymbol{W}_1$.
Case 2
Let $a = 0$. By substituting $x_1 = (cw)^{-1}(\alpha+\beta+c^2)$ into the equation(2), we have a quadratic equation as follows.

$$x_3^2 + (\alpha+\beta+c^2)c^{-1}x_3 + (\alpha+\beta+c^2)^2(cw)^{-2} + \alpha + x_0 \qquad (6)$$

If $\alpha+\beta = c^2$, then the equation(6) has one solution for each $x_0 \in \mathrm{GF}(q)$. If $\alpha+\beta \neq c^2$, then the equation(6) has two solution for $\frac{q}{2}$ $x_0 \in \mathrm{GF}(q)$.

Therefore there are q solutions in domain $\boldsymbol{W}_1$ which satisfy $F_1 = \alpha$, $F_2 = \beta$ for any $\alpha, \beta \in \mathrm{GF}(q)$. □

Theorem 4.4 *Suppose that* $\boldsymbol{W}_2 = L(\pi_1 \setminus l)\}$ *and* $f_1, \ldots, f_k$ *be quadraric functions of* G *respectively. Then* $A(f_1, f_2, \ldots, f_k; \boldsymbol{W}_2)$ *is an* $BA_\lambda(q^2(q-1), q^2, q, 2)$,$q = 2^h$, $h \geq 2$, *with*

$$\lambda(\alpha,\beta) = \begin{cases} 0 & if \;\; \alpha=\beta=0 \\ 1 & if \;\; \alpha=0 \; or \; \beta=0 \\ q & if \;\; \alpha=\beta, \; \beta\neq 0 \\ q+1 & if \;\; \alpha\neq\beta, \; \alpha,\beta\neq 0 \end{cases} \qquad (7)$$

Proof. Similary to Theorem 4.3 , we will show that the number of solutions for $\boldsymbol{x}$ which satisfy $F_1 = \alpha$, $F_2 = \beta$. Since we can put $x_0 = x_2$ on the equations (2), (3) and (4), we have

$$x_1^2 + wx_1x_3 + x_3^2 = \alpha, \qquad (8)$$

$$x_1^2 + cwx_1x_2 + wx_1x_3 + (a^2 + c^2 + acw)x_2^2 + awx_2x_3 + x_3^2 = \beta, \qquad (9)$$

$$x_2(cwx_1 + ux_2 + awx_3) = \alpha + \beta \;\; where\; u = a^2 + c^2 + acw \neq 0. \qquad (10)$$

Consider the following two cases:

Case 1

Let $a \neq 0$. By substituting $x_3 = a^{-1}cx_1 + (aw)^{-1}\{ux_2 + (\alpha+\beta)x_2^{-1}\}$ into the equation(8), we have a quadratic equation as follows.

$$ux_1^2 + \{ux_2 + (\alpha + \beta)x_2^{-1}\}ax_1 + w^{-2}\{ux_2 + (\alpha + \beta)x_2^{-1}\}^2 + a^2\alpha = 0 \quad (11)$$

If $x_2^2 = \frac{\alpha+\beta}{u}$, then the equation(11) has one solution for $\alpha \neq \beta$. If $x_2^2 \neq \frac{\alpha+\beta}{u}$, then the equation(11) has two solutions on condition $D(\delta) = 0$ where $\delta = u/(a^2w^2) + (u\alpha)/\{ux_2 + (\alpha + \beta)x_2^{-1}\}^2$. Since $D(\frac{u}{a^2w^2}) = 1$, we will find the number of x_2 such that $D(\delta') = D(u\alpha/\{ux_2 + (\alpha+\beta)x_2^{-1}\}^2) = 1$. By using Lemma 4.1 ,

$$|\{x_2 \in \mathrm{GF}(q)\,;\, D(\delta') = 1\}| = \begin{cases} 0 & if \quad \alpha = 0 \text{ or } \beta = 0 \\ \frac{q}{2} & if \quad \alpha,\, \beta \neq 0 \end{cases}$$

Therefore the number of solutions which satisfy $F_1 = \alpha$, $F_2 = \beta$ is

$$\begin{cases} 0 & if \quad \alpha = \beta = 0 \\ 1 & if \quad \alpha = 0 \text{ or } \beta = 0 \\ q & if \quad \alpha = \beta,\, \beta \neq 0 \\ q+1 & if \quad \alpha \neq \beta,\, \alpha, \beta \neq 0 \end{cases}$$

.

Case 2

Let $a = 0$. By substituting $x_1 = \{c^2x_2 + (\alpha + \beta)x_2^{-1}\}(cw)^{-1}$ into the equation(8), we have a quadratic equation as follows.

$$x_3^2 + \{c^2x_2 + (\alpha+\beta)x_2^{-1}\}c^{-1}x_3 + \{c^2x_2 + (\alpha+\beta)x_2^{-1}\}^2(cw)^{-2} + \alpha = 0 \quad (12)$$

Then we can prove the number of solutions by similar technique.

From Lemma 4.2, we have the same result for any $F_i = \alpha$, $F_j = \beta$. Therefore $A(f_1, f_2, \ldots, f_k; \boldsymbol{W}_1)$ is an $BA_\lambda(q^3, q^2, q, 2)$ with parameter given in (7). □

References

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

[2] I.M. Chakravarti, *Fractional replication in asymmetrical factorial designs and partially balanced arrays*, Sankhya **17** (1956), 143-164.

[3] J.D. Horton, *Sub-Latin squares and incomplete orthogonal arrays*, J. Combin. Theory Ser. A **16** (1974), 23-33.

[4] M. Jimbo (Private communication).

[5] J.A. Rafter and E. Seiden, *Contributions to the theory and construction of balanced arrays*, Ann. Statest. **2** (1974), 1256-1273.

[6] J.N. Srivastava, *Some general existence conditions for balanced arrays of strength t and 2 symbols*, J. Combin. Theory Ser. A **13** (1972), 198-206.