Mutually M-intersecting Varieties and Combinatorial Arrays

Submitted in Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

in Management Science and Engineering

by

Nobuko Miyamoto

Doctoral Program in Policy and Planning Sciences

University of Tsukuba

January 1998

Abstract

In the design of experiments, combinatorial arrays such as orthogonal arrays and balanced arrays have been used for obtaining proper data with as few experiments as possible. Fractional factorial designs derived from combinatorial arrays offer great economy of time and resources and are used in agricultural, biological and industrial experiments.

A balanced array is an $m \times N$ array A with elements from a set of s symbols such that a t-column vector $(x_1, x_2, \ldots, x_t)^T$ appears $\mu_{x_1,x_2,\ldots,x_t}$ times in any $t \times N$ subarray of A, where $\mu_{x_1,x_2,\ldots,x_t}$ is invariant under any permutation of $x_1, x_2, \ldots, x_t$. If $\mu_{x_1,x_2,\ldots,x_t}$ is constant for all t-vectors, A is called an orthogonal array.

Balanced arrays were introduced by Chakravarti in 1956 as a generalization of orthogonal arrays. The concept of balanced arrays play a key role in the study of several areas of combinatorial theory. For example, the incidence matrices of block designs such as BIB designs and (r, λ)-designs are balanced arrays with proper specifications of the parameters involved.

The problem of construction of balanced arrays except for orthogonal arrays is tough. Although necessary and sufficient conditions for the existence of balanced arrays have been obtained, they do not give any clue as to how to construct balanced arrays in practice. Recently some construction methods have been given by utilizing the structure of block designs. Here a direct construction of balanced arrays by applying the well-known Bose construction of orthogonal arrays is considered. In Chapter 2 a construction of orthogonal arrays which was proposed by Bose in 1947 is generalized. The construction of Bose utilizes linear transformations over a finite field. On the other hand, non-linear functions over a finite field instead of linear transformations are considered and restrictions of the domain of functions are made. Moreover two kinds of quadratic functions are used to construct balanced arrays.

When f is a homogeneous polynomial, the set of points $\mathbf{x}$ on a projective space satisfying $f(\mathbf{x}) = 0$ is called a variety. We are interested in finding a

set of varieties such that each variety contains ρ points and the number of points in the intersection of two distinct varieties is contained in a set M. This is called a set of mutually M-intersecting varieties. When M consists of a singleton, a set of mutually M-intersecting varieties is useful to construct balanced arrays in Chapter 2. In Chapter 3 sets of mutually M-intersecting varieties are constructed by using Hermitian forms.

Acknowledgments

I would like to express my appreciation to my supervisor, Professor Ryoh Fuji-Hara, who has given me strong support and valuable guidance, not only during the preparation of the thesis, but throughout all aspect of my academic career.

I am also very grateful to Professor Shinji Kuriki, Osaka Prefecture University, who offered many helpful suggestion and constant encouragement.

Contents

Notations

The notations, symbols and abbreviations below are used throughout this paper.

$E(y)$: Expectation of y.

$Var(y)$: Variance of y.

$Cov(y_1, y_2)$: Covariance of y_1 and y_2.

$Cov(\mathbf{y})$: Variance-covariance matrix of vector $\mathbf{y}$.

X^T : Transpose of matrix X.

$|S|$: Cardinality of set S.

$S_1 - S_2$: Difference of two sets S_1 and S_2.

$\binom{n}{m}$: Binomial coefficient. As a special case, $\binom{n}{m} = 0$ if and only if $m > n$ or $m < 0$.

$\mathbf{GF}(q)$: A finite field of order q.

$\mathbf{GF}(q)^*$: The non-zero elements of $\mathbf{GF}(q)$, i.e. $\mathbf{GF}(q) \setminus \{0\}$.

$\mathbf{GF}(q)^n$: n-dimensional vector space over $\mathbf{GF}(q)$.

$\mathbf{PG}(n, q)$: n-dimensional projective geometry over $\mathbf{GF}(q)$.

$OA(N, m, s, t)$: Orthogonal array of strength t with N treatment combinations (or assemblies), m constraints, s levels.

$BA(N, m, s, t)$: Balanced array of strength t with N treatment combinations (or assemblies) , m constraints, s levels.

$\mu_{x_1, x_2, \ldots, x_t}$: The number of vectors $(x_1, x_2, \ldots, x_t)^T$ contained in a $t \times N$ array as columns.

$w(l_0, l_1, \ldots, l_{s-1})$: The number of $t \times 1$ column vectors containing l_0 0's, l_1 1's, $\ldots$, l_{s-1} (s-1)'s in a $t \times N$ array.

$V(f)$: Variety.

$\mathcal{V}(\rho, M)$: A set of mutually M-intersecting varieties.

HV : Hermitian variety.

BFF design : Balanced fractional factorial design.

OA : Orthogonal array.

BA : Balanced array.

PBD : Pairwise balanced design.

BIBD : Balanced incomplete block design.

(r, λ)-design with MBN : (r, λ)-design with mutually balanced nested sub-designs.

Chapter 1

Introduction

1.1 Combinatorial Arrays

Fisher (1926) introduced methods of agricultural experiments to obtain required information efficiently which are called *the design of experiments.* Theory and applications of the design of experiments have been extensively developed and they are now established as an area of statistics. In the design of experiments, a *factorial experiment* is popularly used in various fields, for example, agricultural, biological and industrial fields. In factorial experiments, we can estimate the main effects and the interactions between different factors. If all m factors have the same number of levels (s, say), the factorial design is called an s^m *symmetrical factorial design.* Otherwise, it is called an *asymmetrical factorial design.* In an s^m symmetrical factorial design, all possible factor combinations are considered and hence s^m assemblies (treatment combinations) are needed although the designs allow estimation of main effects and all factor interactions. *Fractional factorial designs* were introduced by Yates (1937) to reduce the total number of assemblies. It is said that a good fractional factorial design should posses each of the following features to a reasonable degree. First, it should be economic, i.e. should involve as few assemblies as desired. Secondly, the correlations among the estimates

of various effects should be small, particularly those involving main effects. Thirdly, the variances for the estimates of different main effects, or those for the interactions should not be widely differ from each of them to another. From this point of view, in fractional factorial designs, combinatorial arrays such as orthogonal arrays and balanced arrays are usually used to obtain a good design.

An orthogonal array is an $m \times N$ array A with elements from a set of s symbols such that any $t \times N$ subarray of A has each t-tuple appearing as a column μ times and denoted by $OA(N, m, s, t)$. Here $N = \mu s^t$. Often μ is called the *index* of the array, t the *strength* of the array, m the number of *constraints* and s the number of *levels*. As a generalization of orthogonal arrays, Chakravarti (1956) first introduced balanced arrays. Let A be an $m \times N$ array with elements from a set of s symbols. If every t-column vector $(x_1, x_2, \ldots, x_t)^T$ appears $\mu_{x_1,x_2,\ldots,x_t}$ times in any $t \times N$ subarray of A and $\mu_{x_1,x_2,\ldots,x_t}$ is invariant under any permutation of $x_1, x_2, \ldots, x_t$, the array A is called a *balanced array* and denoted by $BA(N, m, s, t)$.

Fisher (1926) also utilized the *Latin square design*, which was used for comparing s treatments in s rows and s columns, where rows and columns represent two blocking factors. The Latin square of order s is an arrangement of s Latin letters in a square of s rows and s columns such that every Latin letter occurs once in each row and once in each column. Other extensions of the Latin square design using more than two blocking factors lead to designs in the form of *mutually orthogonal Latin squares*. Two Latin squares are said to be *orthogonal* if superimposing one on the other gives a square with every possible ordered pair occurring exactly once. Before the use of Latin squares as the experimental design, Euler (1782) has investigated Latin squares and their properties as a combinatorial problem. Euler's conjecture that two orthogonal Latin squares of order $4t + 2$ do not exist was very famous. This was disproved for $t \geq 2$ by Bose, Shrikhande and Parker (1960). It is known that the existence of $m - 2$ mutually orthogonal Latin squares of order s

is equivalent to the existence of an $OA(s^2, m, s, 2)$ of index unity (see Hall, 1986).

Here examples of fractional factorial designs are illustrated by utilizing an orthogonal array and a balanced array. Let F_1, F_2, F_3 and F_4 be four factors occurring at two levels (0 and 1, say). Then the following linear fixed effects model is considered.

$$\begin{cases} y_{ijkl} = \mu + \alpha_i + \beta_j + \gamma_k + \delta_l + \varepsilon_{ijkl} \quad (i, j, k, l = 0 \text{ or } 1), \\ \alpha_0 + \alpha_1 = 0,\ \beta_0 + \beta_1 = 0,\ \gamma_0 + \gamma_1 = 0,\ \delta_0 + \delta_1 = 0, \end{cases}$$

where y_{ijkl} denotes an observation for the ith, jth, kth and lth level of F_1, F_2, F_3 and F_4, respectively, μ is an overall mean, α_i and β_j are main effects of the ith level of F_1 and the jth level of F_2, respectively, so γ_k and δ_l are. It is assumed that ε_{ijkl} are random variables with $E(\varepsilon_{ijkl}) = 0$, $Var(\varepsilon_{ijkl}) = \sigma^2$ and are uncorrelated for i, j, k and l.

First, we use the following $OA(8, 4, 2, 2)$ of index 2 for an experiment.

F_1	0	0	0	0	1	1	1	1
F_2	0	0	1	1	0	0	1	1
F_3	0	1	0	1	0	1	0	1
F_4	0	1	1	0	1	0	0	1
	y_1	y_2	y_3	y_4	y_5	y_6	y_7	y_8

Assume that the ith row of the array corresponds to factor F_i and the jth column corresponds to observation y_j. Then the linear model based on the above orthogonal array is given by

$$\mathbf{y} = E\boldsymbol{\theta} + \boldsymbol{\varepsilon},$$

where

$$\mathrm{y} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \end{bmatrix}, \; E = \begin{bmatrix} 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}, \; \boldsymbol{\theta} = \begin{bmatrix} \mu \\ \alpha_1 \\ \beta_1 \\ \gamma_1 \\ \delta_1 \end{bmatrix}, \; \boldsymbol{\varepsilon} = \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \varepsilon_3 \\ \varepsilon_4 \\ \varepsilon_5 \\ \varepsilon_6 \\ \varepsilon_7 \\ \varepsilon_8 \end{bmatrix}.$$

Since $\alpha_0 + \alpha_1 = 0$, the main effect α_0 can be expressed by $-\alpha_1$. Hence the entries of E are denoted by -1 or 1 according to the corresponding levels of factors. Here E is called a *design matrix* and $M = E^T E$ is called an *information matrix*. If M is nonsingular, the best linear unbiased estimate of $\boldsymbol{\theta}$ and its covariance matrix are given, respectively, by

$$\hat{\boldsymbol{\theta}} = M^{-1} E^T \mathrm{y} \text{ and } Cov[\hat{\boldsymbol{\theta}}] = \sigma^2 M^{-1}.$$

The information matrix of the above example is shown to be $M = 8I_5$. Here I_5 denotes the identity matrix of order 5. Since M is a diagonal matrix, it is easy to compute the estimate $\hat{\boldsymbol{\theta}}$ of $\boldsymbol{\theta}$ and its covariance matrix $(\sigma^2/8)I_5$. Hence the estimate of $\boldsymbol{\theta}$ are all uncorrelated.

Secondly, we use a $BA(8, 4, 2, 2)$ with indices $\mu_{0,0} = 1$, $\mu_{0,1} = 2$ and $\mu_{1,1} = 3$ similarly.

F_1	0	0	0	1	1	1	1	1
F_2	0	1	1	0	0	1	1	1
F_3	1	0	1	0	1	0	1	1
F_4	1	1	0	1	0	0	1	1
	y_1	y_2	y_3	y_4	y_5	y_6	y_7	y_8

The linear fixed effects model based on the above balanced array is given by

$$\mathbf{y} = E\boldsymbol{\theta} + \boldsymbol{\varepsilon},$$

where

$$\mathbf{y} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \end{bmatrix}, \; E = \begin{bmatrix} 1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}, \; \boldsymbol{\theta} = \begin{bmatrix} \mu \\ \alpha_1 \\ \beta_1 \\ \gamma_1 \\ \delta_1 \end{bmatrix}, \; \boldsymbol{\varepsilon} = \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \varepsilon_3 \\ \varepsilon_4 \\ \varepsilon_5 \\ \varepsilon_6 \\ \varepsilon_7 \\ \varepsilon_8 \end{bmatrix}.$$

Then the following symmetric information matrix is obtained:

$$M = \begin{bmatrix} 8 & 2 & 2 & 2 & 2 \\ & 8 & & \mathbf{0} & \\ & & 8 & & \\ & \text{sym.} & & 8 & \\ & & & & 8 \end{bmatrix} = \begin{bmatrix} m_0 & m_1 & m_1 & \cdots & m_1 \\ & m_0 & m_2 & \cdots & m_2 \\ & & m_0 & \ddots & \vdots \\ & \text{sym.} & & m_0 & m_2 \\ & & & & m_0 \end{bmatrix},$$

where $m_0 = \mu_{0,0} + 2\mu_{0,1} + \mu_{1,1}$, $m_1 = -\mu_{0,0} + \mu_{1,1}$ and $m_2 = \mu_{0,0} - 2\mu_{0,1} + \mu_{1,1}$. Although the estimates are not uncorrelated, it holds that $Var(\hat{\alpha}_1) = Var(\hat{\beta}_1) = Var(\hat{\gamma}_1) = Var(\hat{\delta}_1)$ and $Cov(\hat{\alpha}_1, \hat{\mu}) = Cov(\hat{\beta}_1, \hat{\mu}) = Cov(\hat{\gamma}_1, \hat{\mu}) = Cov(\hat{\delta}_1, \hat{\mu})$ and $Cov(\hat{\alpha}_1, \hat{\beta}_1) = Cov(\hat{\beta}_1, \hat{\gamma}_1) = Cov(\hat{\gamma}_1, \hat{\delta}_1)$, etc.

In general, if the effects involving up to l factors are estimable under a design T, a design T is called a *fractional factorial design of resolution* $2l+1$. Moreover a design T is called a *balanced fractional factorial design of resolution* $2l+1$, if M^{-1} is invariant with respect to any permutation of factors. We can say that the previous examples are balanced fractional factorial designs

of resolution III (traditionally written in Roman letters instead of Arabic).

1.2 Balanced Fractional Factorial Designs

The principle of factorial designs was elaborated primarily for agricultural field experiments by Fisher (1926). In factorial experiments, several factors may be investigated simultaneously. Yates (1937) described many designs for factors at two or three levels and introduced fractional factorial designs. A further advance in fractional factorial designs was made by Finney (1945). These designs reduce the total number of assemblies in comparison with the full factorial designs, whereby certain interactions are assumed to be negligible and a selection of all possible assemblies is used. Thus fractional factorial designs offer great economy of time and resources and are used in agricultural, biological and industrial experiments.

Rao (1946) defined hypercubes of strength d which are related to Latin squares and orthogonal Latin squares. Later, Rao (1947) extended the definition of hypercubes of strength d to cover a wider class of arrays called orthogonal arrays. He discussed the use of orthogonal arrays as orthogonal fractional factorial designs which permit the estimation of main effects and interactions up to order $d-1$ when higher order interactions are negligible. Furthermore, Rao (1950) treated the method of construction of orthogonal fractional factorial designs using orthogonal arrays. For some methods of constructions of orthogonal arrays, reference may be made to, for example, Bose (1947), Bose and Bush (1952), Bush (1952b), Addelman and Kempthorne (1961), Seiden (1954), Seiden and Zemach (1966) and others. Some upper bounds on the maximum number of constraints for orthogonal arrays have been obtained by Rao (1947), Bush (1952a), Plackett and Burman (1946) and Bose and Bush (1952).

It is also well known that a necessary and sufficient condition for a 2^m fractional factorial design T of resolution V to be orthogonal is that T is an

orthogonal array of strength 4 (see, for example, Yamamoto, Shirakura and Kuwada (1975)). The term "resolution" of a design was introduced by Box and Hunter (1961), as a means of classifying fractional factorial designs. In orthogonal fractional factorial designs, estimates of main effects and interactions are easily obtained and are all uncorrelated. However, orthogonal fractional factorial designs exist only for special values of parameters and are uneconomic in the sense that they involve more than the desirable number of assemblies.

Balanced arrays were introduced as a generalization of orthogonal arrays and first studied by Chakravarti (1956) (see Section 1.1). Balanced arrays have a key role in the construction of symmetrical and asymmetrical factorial designs and fractionally replicated designs. In comparison to designs derived from orthogonal arrays, for example, designs derivable from balanced arrays require fewer assemblies to accommodate a given number of factors.

The study of balanced arrays was divided into two aspects as Figure 1.1 shows. One concerns the statistical applicability of balanced arrays and the other concerns the construction of balanced arrays. Here the statistical characterization is explained in more detail. Balanced fractional factorial

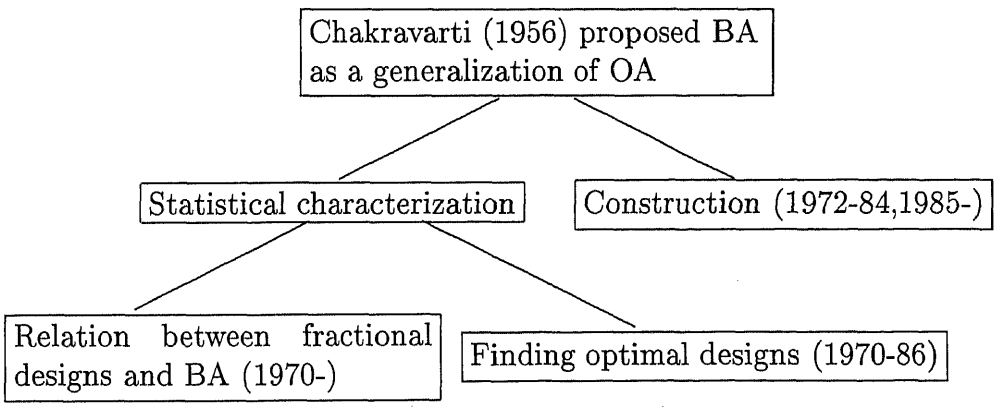

Figure 1.1: History of BA

designs have been investigated by Bose and Srivastava (1964a,b), Srivastava (1970), and Srivastava and Chopra (1971a,b). In particular, Srivastava (1970) has established a connection between a balanced array of strength 4 and a balanced fractional 2^m factorial (briefly, 2^m-BFF) design of resolution V. A general connection between a balanced array of strength $2l$ and a 2^m-BFF design of resolution $2l+1$ has been given by Yamamoto, Shirakura and Kuwada (1975), where $1 \leq l \leq \lfloor \frac{1}{2}m \rfloor$ and $\lfloor x \rfloor$ denotes the greatest integer not exceeding x. Similarly, Kuwada (1979a) has obtained a connection between 3^m-BFF designs of resolution V and 3-symbol balanced arrays of strength 4. Kuwada and Nishii (1979) have also succeeded in establishing a general connection between s^m-BFF designs and s-symbol balanced arrays. Furthermore, Srivastava and Anderson (1970), Shirakura (1975,1976a,1977) and Shirakura and Kuwada (1975,1976) investigated the 2^m-BFF designs of resolution $2l$ and/or $2l+1$ for general l. Hyodo (1992) has established a connection between a simple array, which is a balanced array of strength m, and a 2^m-BFF design of resolution $2l+1$, where $\lfloor \frac{1}{2}m \rfloor < l \leq m$.

By use of the multidimensional partially balanced (MDPB) association scheme (see Bose and Srivastava,1964b) which is a generalization of the ordinary association scheme, the eigenvalues of the information matrix for a 2^m-BFF design of resolution V were obtained by Srivastava and Chopra (1971b). Using the algebraic structure of a triangular multidimensional partially balanced (TMDPB) association scheme, Yamamoto, Shirakura and Kuwada (1976) have obtained an explicit formula for the characteristic polynomial of the information matrix M_T of a 2^m-BFF design T of resolution $2l+1$. This polynomial is useful for comparing designs by the popular criteria such as the trace (A-optimal), the determinant (D-optimal) and the largest root (E-optimal) of M_T^{-1}. For the well-known literature on optimal designs using various criteria, see, for example, Kiefer (1959). A- and/or D-optimal 2^m-BFF designs of resolution V or VII were obtained by Chopra (1975a,b), Chopra and Srivastava (1973a,b,1974,1975), Shirakura (1976b,1977) and Sri-

vastava and Chopra (1971a,1974). More precise tables of A-optimal 2^m-BFF designs in Srivastava and Chopra (1971a) have been presented by Nishii and Shirakura (1986) for $4 \leq m \leq 6$, and Chopra, Kipngeno and Ghosh (1986) for $7 \leq m \leq 10$.

1.3 Block designs

The concept of balanced arrays is related to combinatorial structures of block designs such as pairwise balanced designs, (r, λ)-designs and balanced incomplete block designs. In this section some definitions on block designs are given and a connection between block designs and balanced arrays is presented.

Let V be a finite set of points and $\mathcal{B}$ be a collection of subsets, called *blocks*, of V. Then the pair $(V, \mathcal{B})$ is called a *block design*.

Definition 1.1 (Pairwise Balanced Design, PBD) Let v and λ be positive integers, and K be a set of positive integers greater than one. A (v, K, λ)-PBD is a design $(V, \mathcal{B})$ satisfying the following conditions:

(i) $|V| = v$,

(ii) $|B| \in K$ for every $B \in \mathcal{B}$,

(iii) every pair of distinct points occurs in precisely λ blocks.

If K consists of a single positive integer $k \geq 2$, then a (v, k, λ)-PBD is called a *balanced incomplete block design* (BIBD) and denoted by (v, k, λ)-BIBD. A BIB design is further called a t-(v, k, λ_t) *design*, if each set of t different points occurs together in λ_t blocks. For convenience, let $\lambda_0 = b$ and $\lambda_1 = r$. Thus, a BIBD has five parameters v, b, r, k, λ, which are dependent.

Definition 1.2 ((r, λ)-design) Let r and λ be positive integers such that $r > \lambda$. An (r, λ)-design is a design $(V, \mathcal{B})$ satisfying the following conditions:

(i) every point occurs in precisely r blocks,

(ii) every pair of distinct points occurs in precisely λ blocks.

Note that some blocks of an (r, λ)-design may be empty or singletons. It is obvious that the existence of an (r, λ)-design $(V, \mathcal{B})$ is equivalent to the existence of a $BA(b, v, 2, 2)$ with indices $\mu_{1,1} = \lambda$, $\mu_{0,1} = r - \lambda$ and $\mu_{0,0} = b - 2r + \lambda$, where $b = |\mathcal{B}|$. Kuriki and Fuji-Hara (1994) introduced an (r, λ)-design with mutually balanced nested subdesigns and showed that a connection between the design and a balanced array of strength 2 with s symbols.

Definition 1.3 **((r, λ)-design with MBN)** Let $(V, \mathcal{B})$ be an (r, λ)-design. Suppose that each block $B \in \mathcal{B}$ is partitioned into g subblocks $B_1, B_2, \ldots, B_g$ (some of them may be empty). Denote the collection of the ith subblocks B_i's for each $B \in \mathcal{B}$ by $\mathcal{B}_i$ and $\Pi = \{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_g\}$. An (r, λ)-design with mutually balanced nested subdesigns (for brevity, (r, λ)-design with MBN) is a triple $(V, \mathcal{B}, \Pi)$ satisfying the following conditions:

(i) $(V, \mathcal{B}_i)$ is an (r_i, λ_i)-design for $i = 1, 2, \ldots g$,

(ii) for distinct points x and y of V, the number of blocks B of $\mathcal{B}$ containing x in the ith subblock and y in the jth subblock of B is $\lambda_{i,j}$ which is independent of the x and y chosen.

Note that $\lambda_{i,j} = \lambda_{j,i}$ and $\lambda_i = \lambda_{i,i}$. It is easily seen that

$$r = \sum_{i=1}^{g} r_i \text{ and } \lambda = \sum_{i=1}^{g} \lambda_i + 2 \sum_{1 \le i < j \le g} \lambda_{i,j}.$$

Result 1.1 (Kuriki and Fuji-Hara, 1994) *The existence of an (r, λ)-design $(V, \mathcal{B}, \Pi)$ with mutually balanced nested subdesigns is equivalent to the exis-*

tence of a $BA(b, v, s, 2)$ *with indices*

$$\mu_{i,j} = \begin{cases} \lambda_{i,j}, & \text{if } i \neq j \text{ and } i, j \neq 0, \\ \lambda_i, & \text{if } i = j \neq 0, \\ r_i - \sum_{u=1}^{s-1} \lambda_{i,u}, & \text{if } i \neq 0 \text{ and } j = 0, \\ b - 2r + \lambda, & \text{if } i = j = 0, \end{cases}$$

where $v = |V|$, $b = |\mathcal{B}|$ *and* $s = |\Pi| + 1$.

1.4 History of Constructions

The study of construction of balanced arrays is illustrated in Figure 1.2. It may be mainly classified into two classes, one concerns the existence conditions and another concerns construction methods.

First, the existence conditions are mentioned. Balanced arrays of strength t and $m(\geq t)$ constraints may not exist for an arbitrary set of values of parameters. Necessary and sufficient conditions for the existence of 2-symbol balanced arrays were obtained for $m = t+1$ and $t+2$ by Srivastava (1972) and for $m = t+3$ by Shirakura (1977). Srivastava (1972) also gave some necessary conditions in terms of many systems of Diophantine equations, and Srivastava and Chopra (1973) investigated these necessary conditions extensively. For 3-symbol balanced arrays, Srivastava and Wijetunga (1981) investigated a necessary and sufficient condition for the existence of balanced arrays with $t+1$ constraints. Their results, however, involve several errors to be corrected. For s-symbol balanced arrays, necessary and sufficient conditions for the existence of a balanced array have been obtained for $m = t+1$ by Yamamoto, Kuriki and Yuan (1983), who also corrected Lemma 7.1 of Srivastava and Wijetunga (1981), and for $m \geq t + 2$ by Kuriki (1984a,1984b,1988). For upper bounds on the maximum number of constraints for balanced arrays, refer to Chopra (1982,1983b), Rafter and Seiden (1974), Saha, Mukerjee and Kageyama (1988), and Yamamoto, Kuwada and Yuan (1985).

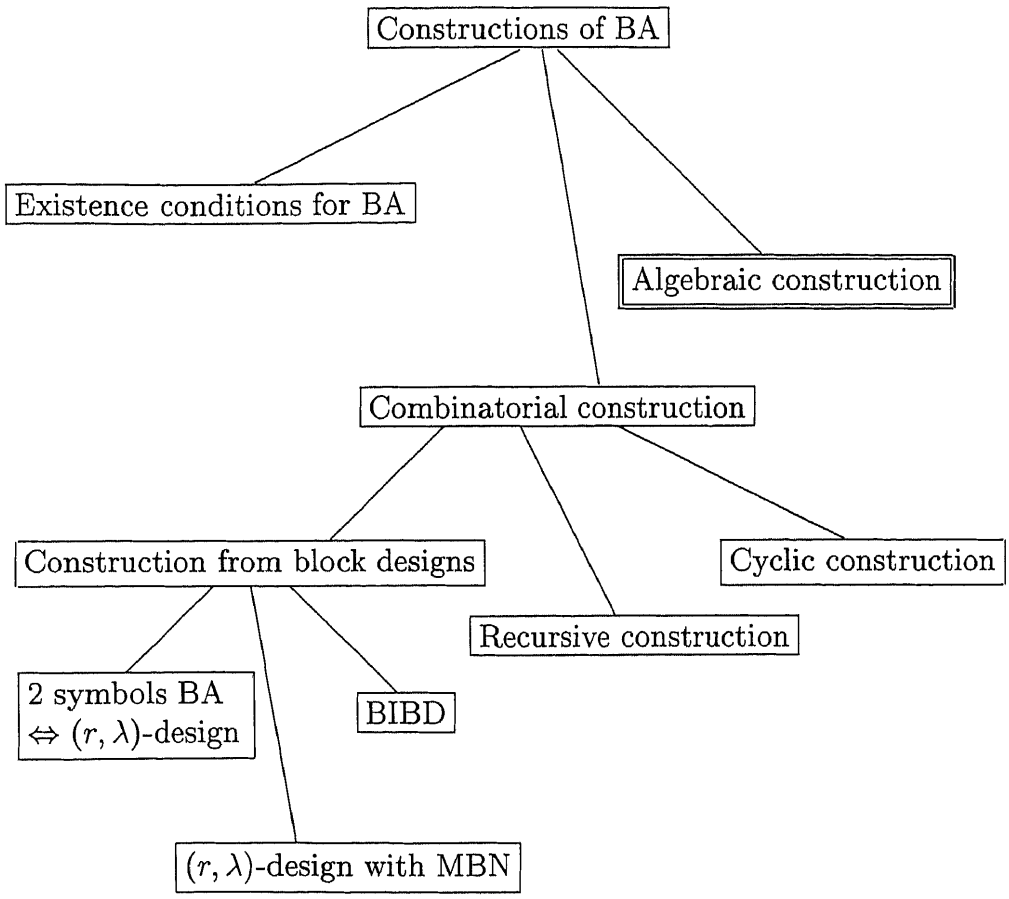

Figure 1.2: Constructions of BA

Secondly, we look at another direction of the study, i.e. finding methods of constructions. Many balanced arrays have been constructed by utilizing combinatorial structure. As mentioned before, block designs are related to balanced arrays. The incidence matrices of a BIBD and an (r, λ)-design are balanced arrays with appropriate specifications of the parameters involved. Moreover, Chakravarti (1961), Rafter and Seiden (1974), Chakravarti and Dey (1976) and Dey, Kulshreshtha and Saha (1972) have given methods of constructing three-symbol balanced arrays of strength two or three by using BIBDs. Kageyama (1975) constructed s-symbol balanced arrays of strength t by generalizing the result of Dey, Kulshreshtha and Saha (1972). Kuriki and Fuji-Hara (1994) showed a connection between (r, λ)-designs with MBN and balanced arrays of strength two. Regarding recursive constructions and cyclic constructions, Fuji-Hara, Jimbo and Yuan (1989) presented a recursive construction method of balanced arrays. A cyclic construction, in which the concept of cyclic code of coding theory is used, was given by Fuji-Hara, Kuriki and Miyake (1996).

In the present thesis, we propose a basic idea of algebraic constructions which has not been investigated before. Orthogonal arrays are usually constructed algebraically by using finite fields. We generalize this construction method of orthogonal arrays to obtain balanced arrays in Chapter 2.

1.5 Known Constructions

In this section, we introduce major results on constructions of balanced arrays studied last forty years. First, existence conditions for balanced arrays are given. For convenience, the following notation of the indices of a balanced array A instead of $\mu_{x_1,x_2,\ldots,x_t}$ is used. Let $w(l_0, l_1, \ldots, l_{s-1})$ denote the number of t-column vectors containing l_0 0's, l_1 1's, $\ldots$, l_{s-1} (s-1)'s in any $t \times n$ subarray. For example, $w(2,0)$, $w(1,1)$ and $w(0,2)$ mean $\mu_{0,0}$, $\mu_{0,1}$ and $\mu_{1,1}$, respectively. Let $\Omega = \{1, 2, \ldots, m\}$ denote the set of row

indices of A and let $I_0, I_1, \ldots, I_{s-2}$, I denote s mutually disjoint subsets of Ω. Let $\nu(I_0, I_1, \ldots, I_{s-2})$ be the number of columns of T with the following entries: in each column, the symbol j occurs at every row of I_j for $j = 0, 1, \ldots, s-2$, and the symbol $s-1$ occurs at the remaining rows. Further let $\nu^*(I_0, I_1, \ldots, I_{s-2}|I)$ be the number of columns of T with the following entries: in each column, the symbol j occurs at every row of I_j for $j = 0, 1, \ldots, s-2$ and the symbol $s-1$ occurs at the remaining rows not in I, whereas at each column in I any symbol from 1 to $s-1$ occurs. The following result gives a general condition for the existence of balanced arrays.

Kuriki (1984b) *A necessary and sufficient condition for the existence of a* $BA(n, m, s, t)$ *is that there exists a set of*

$$\sum_{j=0}^{e-1} \binom{m}{j} (s-1)^{m-j}$$

non negative integers $\nu(J_0, J_1, \ldots, J_{s-2})$ *with* $|J_0| \leq e-1$ *such that, for every family of* $s-1$ *mutually disjoint subsets* I_0 $(|I_0| \geq e)$, $I_1, \ldots, I_{s-2}$ *of* Ω *with respective cardinalities* $e + l_0, l_1, \ldots, l_{s-2}$, $\tilde{\nu}(I_0, I_1, \ldots, I_{s-2})$ *is not greater than or not less than* $\Phi(I_0, I_1, \ldots, I_{s-1})$ *according as* l_0 *is even or odd, where* $e = m - t$,

$$\Phi(I_0, I_1, \ldots, I_{s-1})$$

$$= \sum_{l_0^{(1)}=0}^{l_0} \cdots \sum_{l_0^{(e)}=0}^{l_0^{(e-1)}} (-1)^{l_0^{(e)}} \times \sum_{\substack{l_1^{(1)}, l_2^{(1)}, \ldots, l_{s-1}^{(1)} \geq 0 \\ l_1^{(1)}, l_2^{(1)}, \ldots, l_{s-1}^{(1)} = l_0 - l_0^{(1)}}} \binom{l_0 - l_0^{(1)}}{l_1^{(1)}, l_2^{(1)}, \ldots, l_{s-1}^{(1)}} \cdots$$

$$\times \sum_{\substack{l_1^{(e)}, l_2^{(e)}, \ldots, l_{s-1}^{(e)} \geq 0 \\ l_1^{(e)}, l_2^{(e)}, \ldots, l_{s-1}^{(e)} = l_0^{(e-1)} - l_0^{(e)}}} \binom{l_0^{(e-1)} - l_0^{(e)}}{l_1^{(e)}, l_2^{(e)}, \ldots, l_{s-1}^{(e)}}$$

$$\times w(l_0^{(e)}, l_1 + l_1^{(1)} + \cdots + l_1^{(e)}, \ldots, l_{s-1} + l_{s-1}^{(1)} + \cdots + l_{s-1}^{(e)}),$$

$$\tilde{\nu}(I_0, I_1, \ldots, I_{s-2}) = \sum_{j=0}^{e-1} \binom{l_0 + e - j - 1}{l_0} \sum_{I_0' \in \mathcal{R}_j(I_0)} \nu^*(I_0', I_1, \ldots, I_{s-2} | I_0 - I_0'),$$

$|I_0| = e + I_0$, $|I_j| = l_j$ $(j = 1, 2, \ldots, s-2)$ *and* $\mathcal{R}_j(I)$ *denotes a collection of all subsets of* I *with cardinality* j.

In 2-symbol balanced arrays, the index $w(l_0, l_1)$ is denoted by w_j with $j = l_1$. Shirakura (1977) considered a balanced array of strength m and called it a *simple array*. The above result yields a necessary and sufficient condition for the existence of a simple array.

Kuriki (1993) *A necessary and sufficient condition for the existence of a simple* $BA(n, m, 2, t)$ *is that there exists a non negative integers* $\nu_0, \nu_1, \ldots, \nu_{e-1}$ *such that, for* $l = 0, 1, \ldots, t$,

$$\sum_{j=0}^{e-1} \binom{l + e - j - 1}{l} \binom{l + e}{j} \nu_j$$

is not greater than or not less than $\Phi(l, t - l)$ *according as* l_0 *is even or odd, where*

$$\Phi(l, t - l) = \sum_{l^{(1)}=0}^{l} \cdots \sum_{l^{(e)}=0}^{l^{(e-1)}} (-1)^{l^{(e)}} w_{t - l^{(e)}}$$

and $e = m - t$.

An existence condition for 2-symbol balanced arrays with $t+2$ constraints was given by Srivastava (1972). This condition corresponds to the case $s = 2$ and $e = 2$ in Theorem 2.2 of Kuriki (1984b). An existence condition for simple arrays with $m = t + 2$ can be given by Theorem 2.2 of Kuriki (1993) with $e = 2$.

Srivastava (1972) *A necessary and sufficient condition for the existence of*

a $BA(n, t+2, 2, t)$ *is that there exists a set of* $t+3$ *non negative integers* $\nu(\phi), \nu(1), \ldots, \nu(t+2)$ *such that*

$$\nu(1) \leq \nu(2) \leq \cdots \leq \nu(t+2)$$

and that, for $l = 0, 1, \ldots, t$,

$$\begin{array}{ll} (l+1)\nu(\phi) + \sum_{l'=0}^{l+1} \nu(t-l'+2) \leq \psi_l, & \text{if} \quad l \text{ is even}, \\ (l+1)\nu(\phi) + \sum_{l'=0}^{l+1} \nu(l'+1) \geq \psi_l, & \text{if} \quad l \text{ is odd}, \end{array}$$

where

$$\psi_l = \sum_{l'=0}^{l} (-1)^{l'} (l-l'+1) w_{t-l'}.$$

Here $\nu(\{i\})$ *is denoted by* $\nu(i)$ *for brevity.*

Kuriki (1993) *A necessary and sufficient condition for the existence of a simple* $BA(n, t+2, 2, t)$ *is that there exist two non negative integers* ν_0 *and* ν_1 *such that for* $l = 0, 1, \ldots, t$, $(l+1)\nu_0 + (l+2)\nu_1$ *is not greater than or not less than* ψ_l *according as* l *is even or odd, where* ψ_l *is given by Srivastava* (1972).

For 2-symbol balanced arrays of strength t with $t+2$ constraints, Kuriki (1988) showed that the existence of balanced arrays can be determined by the existence of simple arrays.

Kuriki (1988) *There exists a* $BA(n, t+2, 2, t)$ *if and only if there exists a simple* $BA(n', t+2, 2, t)$ *with indices* w_j' *such that, for some integer* h $(0 \leq h \leq t+1)$,

$$w_j' = w_j - w_j''(h)$$

holds for all $j = 0, 1, \ldots, t$, *where*

$$w_j''(h) = \begin{cases} \min\{t-j+2, h\} - 2\max\{0, h-j-1\} + \min\{t-j, h\}, \\ \qquad\qquad \textit{if } t-j \textit{ is even}, \\ -\max\{0, h-j\} + 2\min\{t-j+1, h\} - \max\{0, h-j-2\}, \\ \qquad\qquad \textit{if } t-j \textit{ is odd}. \end{cases}$$

Furthermore, Kuriki (1988) improved the existence condition for a $BA(n, t+2, 2, t)$ given by Srivastava (1972) as follows.

Kuriki (1988) *A necessary and sufficient condition for the existence of a* $BA(n, t+2, 2, t)$ *is that there exist two non negative integers* ν_0 *and* ν_1 *such that for* $l = 0, 1, \ldots, t$ *and some integer* h $(0 \le h \le t+1)$, $(l+1)\nu_0 + (l+2)\nu_1$ *is not greater than or not less than* ψ_l' *according as* l *is even or odd, where*

$$\psi_l' = \begin{cases} \psi_l - \min\{l+2, h\}, & \textit{if } l \textit{ is even}, \\ \psi_l - \max\{0, h-t+l\}, & \textit{if } l \textit{ is odd}, \end{cases}$$

where ψ_l *is given in Srivastava* (1972).

Secondly, a list of some useful known constructions of balanced arrays is given.

Chakravarti (1961) *There exists a* $BA(b, v, 2, t)$ *with indices* $\mu_{x_1, x_2, \ldots, x_t}$ *and which is obtained from a* t-(v, k, λ_t) *design. When* $x_i = 1$ *for* $i = 1, 2, \ldots, r$ *and* $x_i = 0$ *for* $i = r+1, \ldots, t$,

$$\begin{aligned} \mu_{x_1, x_2, \ldots, x_t} &= \lambda(x_1, x_2, \ldots, x_t) \\ &= \lambda_r - \binom{t-r}{1}\lambda_{r+1} + \binom{t-r}{2}\lambda_{r+2} - \cdots + (-1)^{t-r}\binom{t-r}{t-r}\lambda_t, \end{aligned}$$

where $\lambda_0 = b$, $\lambda_1 = r$.

Kageyama (1975) *There exists a* $BA(2b, v, 3, t)$ *with indices*

$$\mu_{x_1,x_2,\ldots,x_t} = \begin{cases} \lambda(x_1, x_2, \ldots, x_t), & \text{if } x_i = 0 \text{ or } 1 \text{ for } i = 1, 2, \ldots, t, \\ \lambda(\varepsilon(x_1), \varepsilon(x_2), \ldots, \varepsilon(x_t)), & \text{if } x_i = 1 \text{ or } 2 \text{ for } i = 1, 2, \ldots, t, \\ \quad \text{where } \varepsilon(1) = 1 \text{ and } \varepsilon(2) = 0 & \\ 2\lambda_t, & \text{if } x_i = 1 \text{ for all } i = 1, 2, \ldots, t, \\ 0, & \text{if } x_i = 0 \text{ and } x_j = 2 \text{ for some } i, j = 1, 2, \ldots, t, \end{cases}$$

where $\lambda(x_1, x_2, \ldots, x_t)$ *is given in Chakravarti* (1961).

The cases that $t = 2$ and $t = 3$ in the above result were given in Dey, Kulshreshtha and Saha (1972).

Rafter and Seiden (1976) *There exists a* $BA(b - r, r, k, 2)$ *with indices*

$$\mu_{i,j} = \begin{cases} 1, & \text{if } i, j \neq 0, \\ r - k, & \text{if } i \neq 0 \text{ and } j = 0, \\ b - r - (k-1)(2r - k - 1), & \text{if } i = j = 0, \end{cases}$$

which is obtained from a $(v, k, 1)$*-BIBD with the usual parameters* r, b.

Chakravarti and Dey (1976) *There exists a* $BA(8t + 6, 4t + 3, 3, 2)$ *with indices* $\mu_{0,0} = \mu_{2,2} = t$, $\mu_{0,1} = \mu_{1,2} = t + 1$, $\mu_{1,1} = 2t$ *and* $\mu_{0,2} = 1$.

Chakravarti and Dey (1976) *There exists a* $BA(8t + 2, 4t + 1, 3, 2)$ *with indices* $\mu_{0,0} = \mu_{1,1} = 2t - 1$, $\mu_{0,1} = 2t$, $\mu_{0,2} = \mu_{1,2} = 1$ *and* $\mu_{2,2} = 0$.

Kuriki and Fuji-Hara (1994) *There exists a* $BA((s-1)(s-2)b, v, s, 2)$

with indices

$$\mu_{i,j} = \begin{cases} \lambda - \lambda', & \text{if } i \neq j \text{ and } i, j \neq 0, \\ (s-2)\lambda', & \text{if } i = j \neq 0, \\ (s-2)(r-\lambda), & \text{if } i \neq 0 \text{ and } j = 0, \\ (s-1)(s-2)(b-2r+\lambda), & \text{if } i = j = 0, \end{cases}$$

which is obtained from an (r, λ)*-design* $(V, \mathcal{B}, \Pi)$ *with MBN, where* $|V| = v$, $|\mathcal{B}| = b$, $|\Pi| = s-1$, $r_i = s-2$, $\lambda_i = (s-2)\lambda'$, $\lambda_{i,j} = \lambda - \lambda'$ *and* λ' *is the number of blocks of* Π *containing any pair of distinct points of* V.

Kuriki and Fuji-Hara (1994) *There exists a* $BA(q^d(q^{d-d'}-1), \phi(n-1, d'-1, q), q^{d-d'}+1, 2)$ *with indices*

$$\mu_{i,j} = \begin{cases} \{q^{d'}/(q^{d'}-1)\}\Phi, & \text{if } i \neq j \text{ and } i, j \neq 0, \\ \Phi, & \text{if } i = j \neq 0, \\ q^d\Phi & \text{if } i \neq 0 \text{ and } j = 0, \\ q^{d-d'}(q^n - q^d - 1), & \text{if } i = j = 0, \end{cases}$$

for a prime power q *and all positive integers* d *and* d' *such that* $d > d'$, *where* $n = d + d'$, $\Phi = (q^{d-d'}-1)\phi(n-2, d'-2, q)$, *and*

$$\phi(n-1, d-1, q) = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-d+1}-1)}{(q^d-1)(q^{d-1}-1)\cdots(q-1)}.$$

Kuriki and Fuji-Hara (1994) *There exists a* $BA(pv, v, s, 2)$ *with indices*

$$\mu_{i,j} = \begin{cases} fl_il_j, & \text{if } i \neq j \text{ and } i, j \neq 0, \\ l_i(fl_i - 1), & \text{if } i = j \neq 0, \\ l_i\{f(p-l)+1\} & \text{if } i \neq 0 \text{ and } j = 0, \\ (p-l)\{f(p-l)+1\} & \text{if } i = j = 0, \end{cases}$$

for a prime power $v = pf + 1$, *where* $l_1, l_2, \ldots, l_{s-1}$ *are positive integers such that* $l = \sum_{i=1}^{s-1} \leq p$.

In any column $(x_1, x_2, \ldots, x_m)^T$ of a balanced array A, if A contains $(x_m, x_1, \ldots, x_{m-1})^T$, A is said to be *cyclic*.

Fuji-Hara, Kuriki and Miyake (1996) *There exists a cyclic* $BA((p\lambda_0 n + p')nv, nv, s, 2)$ *with indices*

$$\mu_{i,j} = \begin{cases} \lambda_0 f l_i l_j, & \text{if } i \neq j \text{ and } i, j \neq 0, \\ \lambda_0 l_i (f l_i - 1), & \text{if } i = j \neq 0, \\ \lambda_0 (nv - fl) l_i & \text{if } i \neq 0 \text{ and } j = 0, \\ (p\lambda_0 - 2\lambda_0 l + p')nm + \lambda_0 l(fl + 1), & \text{if } i = j = 0, \end{cases}$$

for odd prime powers $v = pf + 1$ *and* $n = p'f' + 1$, *where* $l_1, l_2, \ldots, l_{s-1}$, $l'_1, l'_2, \ldots, l'_{s-1}$, λ_0 *are positive integers such that* $l = \sum_{i=1}^{s-1} l_i \leq p$, $\sum_{i=1}^{s-1} l'_i \leq p'$, $f = \lambda_0 f'$ *and* $l'_i = \lambda_0 l_i$ *for* $i = 1, 2, \ldots s-1$.

Fuji-Hara, Kuriki and Miyake (1996) *There exists a cyclic* $BA(pv^2(v^h - 1)/(v-1), v^h, s, 2)$ *with indices*

$$\mu_{i,j} = \begin{cases} f l_i l_j, & \text{if } i \neq j \text{ and } i, j \neq 0, \\ l_i (f l_i - 1), & \text{if } i = j \neq 0, \\ (v^h - fl) l_i & \text{if } i \neq 0 \text{ and } j = 0, \\ pv^2(v^h - 1)/(v-1) - 2lv^h + l(fl+1), & \text{if } i = j = 0, \end{cases}$$

for an odd prime powers $v = pf + 1$, *where* $l_1, l_2, \ldots, l_{s-1}$ *are positive integers such that* $l = \sum_{i=1}^{s-1} l_i \leq p$.

At last, a recursive construction of balanced arrays is given. A balanced array A of strength t can be expressed in terms of block designs. A balanced array of strength t is an incidence structure $(V, \mathcal{G}, \mathcal{B})$ which satisfies the

following conditions:

(i) V is a set of kg points.

(ii) $\mathcal{G}$ is a partition of V into k subsets with g points, called *groups*. The point set V may be denoted by $V = \{< i, q > | i \in N_k, q \in N_g\}$, where $N_f = \{1, 2, \ldots, f\}$.

(iii) $\mathcal{B}$ is a collection of k-subsets, called *blocks*, of V each containing exactly one point from each group.

(iv) For any $i_1, i_2 \in N_k$ $(i_1 \neq i_2)$, $q_1, q_2 \in N_g$, there are exactly $\eta(q_1, q_2)$ blocks containing a pair of points $< i_1, q_1 >$ and $< i_2, q_2 >$. Here $\eta(q_1, q_2)$ is independent of the choice of i_1 and i_2 and is called an *index function*.

A balanced array of strength two is also denoted by $BA_\eta[k; g]$. If $\eta(q_1, q_2) = \mu$ for all $q_1, q_2 \in N_g$, $BA_\eta[k; g]$ is further called a transversal design $TD_\mu[k; g]$.

Fuji-Hara, Jimbo and Yuan (1989) *Let $A = (V, \mathcal{G}, \mathcal{B})$ be a $BA_\eta[k + l; g]$ with group set $\mathcal{G} = \{G_1, \ldots, G_k; H_1, \ldots, H_l\}$. Let S be an s-subset of $H_1 \cup H_2 \cup \cdots \cup H_l$ and $u_B = |B \cap S|$ for each block $B \in \mathcal{B}$. Denote $\{u_B | B \in \mathcal{B}\}$ by $\{u_j | u_1 < u_2 < \cdots < u_d\}$. Assume the existence of $BA_{\eta_j}[k; m + u_j]$'s for $j = 1, 2, \ldots, d$, where η_j is the index function satisfying the following conditions:*

a) $\eta_j(p, q) = \eta_{j+1}(p, q)$ *for any* $p, q \in N_{m+u_j}$,

b) $\eta_d(p, q_1) = \eta_d(p, q_2)$ *for all* $p \in N_m$, $q_1, q_2 \in N_{m+u_d} \setminus L_m$,

c) $\eta_d(p_1, q_1) = \eta_d(p_2, q_2)$ *for any* $P_1, p_2, q_1, q_2 \in N_{m+u_d} \setminus N_m$, $(p_1 \neq q_1, p_2 \neq q_2)$,

d) $\eta_d(p, p) = \eta_d(q, q)$ *for any* $p, q \in N_{m+u_d} \setminus N_m$.

Then there exists a $BA_{\eta^*}[k; mg+s]$ *with an index function* η^**, where*

$$\eta^*((x,p),(y,q)) = \eta(x,y)\eta_d(p,q) \quad \textit{if} \quad (x,p),(y,q) \in N_g \times N_m,$$
$$\eta^*((x,p),s') = \eta(x,y)\eta_d(p,q) \quad \textit{if} \quad (x,p) \in N_g \times N_m,\ s' =< v,y >\in S,$$
$$(q \in N_{m+u_d} \setminus N_m),$$
$$\eta^*(s',s'') = \eta(x,y)\eta_d(p,q) \quad \textit{if} \quad s' =< u,x >, s'' =< v,y >\in S,\ u \neq v,$$
$$(p,q \in N_{m+u_d} \setminus N_m, p \neq q),$$
$$\eta^*(s',s'') = 0 \quad \textit{if} \quad s' =< u,x >, s'' =< v,y >\in S, x \neq y,$$
$$\eta^*(s',s'') = \textstyle\sum_{z\in N_g} \eta(x,z)\eta_d(p,p) \quad \textit{if} \quad s' =< u,x >\in S,\ (p \in N_{m+u_d} \setminus N_m).$$

The above result can be generalized to a case of balanced arrays of strength t (see Fuji-Hara, Jimbo and Yuan, 1989).

Chapter 2

Construction of Balanced Arrays

Bose (1947) proposed a construction of orthogonal arrays. The construction uses linear transformations over a finite field (see Result 2.3). Fuji-Hara and Miyamoto (1995) generalized this method by considering non-linear functions, i.e. elliptic or hyperbolic, instead of linear transformations to construct combinatorial arrays such as orthogonal arrays and balanced arrays. In particular, Fuji-Hara and Miyamoto (1995) constructed combinatorial arrays by using quadratic functions over finite fields of even prime power orders. This method was generalized for prime power orders by Fuji-Hara and Miyamoto (1997a).

2.1 Geometric properties

Some definitions and properties about the finite projective geometries for constructions of combinatorial arrays are presented in this section. Notations and symbols are due to Hirschfeld (1979, 1985), and Hughes and Piper (1973).

An incidence structure is defined by a triple $(V, \mathcal{B}, I)$, where V, $\mathcal{B}$, I are sets with $I \subseteq V \times \mathcal{B}$. The elements of V are called *points*, those of $\mathcal{B}$ *lines*.

If $(p, B) \in I$ for $p \in V$ and $B \in \mathcal{B}$, then it is said that p is incident with B, or B is incident with p, or p lies on B, or B contains p. Of course block designs $(V, \mathcal{B})$ themselves are incidence structures, although we omit I from the notation $(V, \mathcal{B}, I)$.

The incidence structure of a projective plane is first reviewed.

Definition 2.1 An incidence structure $\mathcal{P} = (V, \mathcal{B}, I)$ is called a *projective plane* if and only if the following axioms are satisfied:

(i) any two distinct points are incident with a unique common line;

(ii) any two distinct lines are incident with a unique common point;

(iii) $\mathcal{P}$ contains a set of four points with the property that no three of them lie on a common line.

In particular, when V and $\mathcal{B}$ are finite sets, $\mathcal{P}$ is called a *finite projective plane.* The following result is shown in Hughes and Piper (1973).

Result 2.1 *Let $\mathcal{P} = (V, \mathcal{B}, I)$ be a finite projective plane. There exists a positive integer $n \geq 2$, which is called the* order *of $\mathcal{P}$, such that*

1. *each line contains exactly $n + 1$ points,*

2. *each points lies on exactly $n + 1$ lines,*

3. *$\mathcal{P}$ contains $n^2 + n + 1$ points and $n^2 + n + 1$ lines.*

A projective plane can be constructed as follows. Let V be a 3-dimensional vector space over $\mathbf{GF}(q)$. Choose as a set of points V all 1-dimensional subspaces and as a family of lines $\mathcal{B}$ all 2-dimensional subspaces of V. Then the incidence structure $(V, \mathcal{B}, I)$ is a finite projective plane of order q and denoted by $\mathbf{PG}(2, q)$. Note that a projective plane is not necessarily $\mathbf{PG}(2, q)$. There are projective planes non-isomorphic to $\mathbf{PG}(2, q)$.

Secondly, an *n-dimensional projective geometry* $\mathbf{PG}(n, q)$ over $\mathbf{GF}(q)$ is defined. Let V be an $(n+1)$-dimensional vector space over $\mathbf{GF}(q)$. The one-,

two-, three- and n-dimensional subspaces of V are called a *point*, *line*, *plane*, and *hyperplane* of $\mathbf{PG}(n,q)$, respectively. In general, the $(r+1)$-dimensional subspaces are called *r-flats*. For any two distinct points p and q in an r-flat, all points on the line through p and q are also contained in the r-flat. A projective geometry is the system of all flats satisfying the conditions given in Definition 2.1. For $n > 2$, all projective geometries are isomorphic.

The set of r-flats of $\mathbf{PG}(n,q)$, written by $\mathbf{PG}^{(r)}(n,q)$, is examined. Recall the definition of $\phi(n;\ r,q)$ in Kuriki and Fuji-Hara (1994) in Chapter 1, i.e.

$$\phi(n,r,q) = \frac{(q^{n+1}-1)(q^n-1)\cdots(q^{n-r+1}-1)}{(q^{r+1}-1)(q^r-1)\cdots(q-1)}.$$

Result 2.2

1. *The number of points in* $\mathbf{PG}(n,q)$ *is* $\phi(n,0,q)$.
2. $|\mathbf{PG}^{(r)}(n,q)| = \phi(n,r,q)$.
3. *The number of r-flats through an s-flat in* $\mathbf{PG}(n,q)$ *is* $\phi(n-s-1, n-r-1, q)$.

Next define a set of points which is called a variety or quadric as follows.

Definition 2.2 (Variety) Let f be a homogeneous polynomial. Then the set of all points $\mathbf{x}$ of $\mathbf{PG}(n,q)$ satisfying $f(\mathbf{x}) = 0$ is called a *variety* and denoted by $V(f)$.

In $\mathbf{PG}(n,q)$, all points are represented by $(n+1)$-column vectors $\mathbf{x}$. Let f be a quadratic form, that is, $f(\mathbf{x}) = \mathbf{x}^T\mathbf{Q}\mathbf{x}$, where $\mathbf{x} \in \mathbf{PG}(n,q)$ and $\mathbf{Q}$ is a triangular matrix of order $n+1$ over $\mathbf{GF}(q)$. Then the variety $V(f)$ is called a *quadric*. If there does not exist a non-singular transformation $\mathbf{x} = \mathbf{B}\mathbf{y}$ which will transform a quadric to the form

$$\sum_{i=0, j\geq i}^{l} c_{ij}y_iy_j \quad \text{where } l < n+1 \text{ and } c_{ij} \in \mathbf{GF}(q),$$

then a quadric is said to be *non-degenerate*, otherwise a quadric is called *degenerate.*

For q odd, a triangular matrix $\mathbf{Q}$ is transformed to a symmetric matrix $\mathbf{T}$ of order $n+1$ over $\mathbf{GF}(q)$. Hence a quadric which is defined by $\mathbf{x}^T\mathbf{Tx}$ is non-degenerate if and only if $\mathbf{T}$ is a non-singular matrix on $\mathbf{GF}(q)$.

Non-degenerate quadrics in $\mathbf{PG}(3,q)$ are here considered to utilize the present construction method:

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

(1) for q even, $d \in \{t \in \mathbf{GF}(2^h)\ ;\ D(t) = t + t^2 + \cdots + t^{2^h-1} = 1\}$,

(2) for q odd, $d \in \{t \in \mathbf{GF}(q)\ ;\ 1 - 4t$ is a non-square $\}$.

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

Throughout this thesis, d is used in the above meaning. Finally a bijection over $\mathbf{PG}(n,q)$ is defined.

Definition 2.3 (projectivity) When S and S' are two spaces of $\mathbf{PG}(n,q)$, then a *projectivity* $\alpha : S \to S'$ is a bijection given by matrix $\mathbf{T}$ in the sense that if $P' = P^\alpha$, then $t\mathbf{x}' = \mathbf{Tx}$, where $\mathbf{x}'$ and $\mathbf{x}$ are vector representations of points P' and P respectively, and t is a non-zero element of $\mathbf{GF}(q)$.

A projectivity preserves incidence structure of points and lines; that is, if a point P on l, then P^α on l^α.

2.2 A Generalization of Bose's Construction

A balanced array was first introduced by Chakravarti (1956) in connection with some class of statistical designs as follows.

Definition 2.4 (Balanced array) 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 $BA(N, m, s, t)$ is an $m \times N$ array $\mathbf{A}$ whose elements are from S satisfying the following conditions:

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

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

Here m is called the number of *constraints*, s the number of *levels*, t the *strength* and $\mu_{\mathbf{x}}$ the *indices* of the array. If $\mu_{\mathbf{x}} = \mu$ for every $\mathbf{x} \in S^t$, then the array is called an *orthogonal array* of strength t, and denoted by $OA(N, m, s, t)$, where $N = \mu s^t$.

As a special case of balanced arrays, Horton (1974) defined an incomplete orthogonal array satisfying the conditions (i') below and (ii), denoted by $IOA(N, m, s, h, t)$. Let H be a h-subset of S and H^t the set of all t-dimensional column vectors over H.

(i') in any t-rowed subarray $\mathbf{A}_0$ of $\mathbf{A}$, every $\mathbf{x} \in S^t \setminus H^t$ appears $\mu_{\mathbf{x}}$ times in A_0 and every $\mathbf{x} \in H^t$ appears no times in A_0.

In order to construct balanced arrays, a construction method of orthogonal arrays, proposed by Bose (1947), will be generalized by using multivariate functions and restricting a domain of the functions.

Result 2.3 (The construction of Bose) *Let* $\mathbf{G}$ *be an* $m \times n$ *matrix over* $\mathbf{GF}(q)$*, a finite field of order* q*. If any* t *rows of* $\boldsymbol{G}$ *are linearly independent, then the* m*-dimensional column vector space* $\{\boldsymbol{G}\mathbf{x}\,;\, \mathbf{x} \in \mathbf{GF}(q)^n\}$ *is an* $OA(q^n, m, q, t)$ *with* $\mu = q^{n-t}$.

We consider the linear combination $\mathbf{g}^T\mathbf{x}$ as a linear function $f(\mathbf{x}) = g_1x_1 + g_2x_2 + \cdots + g_nx_n$ where $\mathbf{g} = (g_1, g_2, \ldots, g_n)^T$, $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$. Then

we interpret the method of Bose as follows. For all $\mathbf{x} \in \mathbf{GF}(q)^n$,

$$\mathbf{Gx} = \begin{pmatrix} f_1(\mathbf{x}) = g_{11}x_1 + g_{12}x_2 + \cdots + g_{1n}x_n \\ f_2(\mathbf{x}) = g_{21}x_1 + g_{22}x_2 + \cdots + g_{2n}x_n \\ \vdots \\ f_m(\mathbf{x}) = g_{m1}x_1 + g_{m2}x_2 + \cdots + g_{mn}x_n \end{pmatrix},$$

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

Moreover this method will be generalized by letting $f_1, f_2, \ldots, f_m$ be distinct multivariate functions with a domain $\mathbf{W}$ ($\subseteq \mathbf{GF}(q)^n$) in common, and taking the collection A as

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

denoted by $A(f_1, f_2, \ldots, f_m; \mathbf{W})$. This may be regarded as an array consisting of an arbitrary juxtaposition of column vectors.

Some constructions are first given by restricting a domain $\mathbf{W}$ and letting f_i be linear functions.

Theorem 2.1 *Let* $\mathbf{W}$ *be* $\mathbf{GF}(q^n)^t - \mathbf{GF}(q)^t$ *and* $f_1, f_2, \ldots, f_m$ *be linear functions over* $\mathbf{GF}(q)$, *where any* t *functions of them are independent. Then* $A(f_1, f_2, \ldots, f_m; \mathbf{W})$ *is an* $IOA(q^{nt} - q^t, m, q^n, q, t)$ *with* $\mu = 1$.

Proof. It will be shown that $A(f_1, f_2, \ldots, f_m; \mathbf{W})$ contains every t-column vector from $\mathbf{GF}(q^n)^t - \mathbf{GF}(q)^t$ precisely once. First, we consider a domain $\mathbf{W}$ as $\mathbf{GF}(q^n)^t$. Let $(a_1, a_2, \ldots, a_t)^T$ be a t-vector from $\mathbf{GF}(q^n)^t$. Since

$f_1, f_2, \ldots, f_t$ are linearly independent, the number of solutions $\mathbf{x}$ which satisfy

$$\begin{pmatrix} f_1(\mathbf{x}) \\ f_2(\mathbf{x}) \\ \vdots \\ f_t(\mathbf{x}) \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_t \end{pmatrix}$$

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

Theorem 2.2 *Let* $\mathbf{W}$ *be a hyperplane* $\mathcal{H}$ *of* $\mathbf{GF}(q)^n$ *and let* $f_1, f_2, \ldots, f_m$ *be linear functions, and the intersection of null spaces of any two* f_i,f_j $(i \neq j)$ *is not parallel to* $\mathcal{H}$. *Then* $A(f_1, f_2, \ldots, f_m; \mathbf{W})$ *is an* $OA(q^{n-1}, m, q, 2)$ *with* $\mu = q^{n-3}$.

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

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

for any $a, b \in \mathbf{GF}(q)$ forms an $(n-3)$-dimensional subspace over $\mathbf{GF}(q)$. Hence the cardinality of the set is q^{n-3}. ■

2.3 Generation of non-linear functions

In $\mathbf{PG}(3,q)$, all points are represented by 4-tuples $\mathbf{x} = (x_0, x_1, x_2, x_3)^T$, where $x_i \in \mathbf{GF}(q)$ for $0 \leq i \leq 3$. The 4-tuples $t\mathbf{x} = (tx_0, tx_1, tx_2, tx_3)^T$ is regarded as the same point as $\mathbf{x}$ for any nonzero $t \in \mathbf{GF}(q)^*$ in $\mathbf{PG}(3,q)$. Recall (Definition 2.3) that a projectivity $\alpha : \mathbf{PG}(3,q) \to \mathbf{PG}(3,q)$ is a bijection given by a matrix $\mathbf{T}$ of order 4 over $\mathbf{GF}(q)$.

We consider non-degenerate quadrics in $\mathbf{PG}(3,q)$, which have the canonical forms: $V(dx_0^2 + x_0x_1 + x_1^2 + x_2x_3)$ (for an elliptic quadric) and $V(x_0x_1 + x_2x_3)$ (for a Hyperbolic quadric) (see Section 2.1). An elliptic quadric and a hyperbolic quadric consist of q^2+1 and $(q+1)^2$ points in $\mathbf{PG}(3,q)$, respectively. If a plane of $\mathbf{PG}(3,q)$ 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.

When $A(f_1, f_2, \ldots, f_m; \mathbf{W})$ is a balanced array of strength 2, $\mathbf{x} \in S^2$ appears $\mu_{\mathbf{x}}$ times in any 2-rowed subarray of $A(f_1, f_2, \ldots, f_m; \mathbf{W})$. Hence we can obtain a necessary condition for the existence of a balanced array using varieties.

Theorem 2.3 *Suppose the cardinalities of $V(f_i)$ in $\mathbf{W}$ are the same for all i. If $A(f_1, f_2, \ldots, f_m; \mathbf{W})$ is a balanced array of strength 2, then $|V(f_i) \cap V(f_j)|$ in $\mathbf{W}$ is constant independently of i, j, $i \neq j$ chosen.*

Proof. For $1 \leq i, j \leq m$ and $i \neq j$, $|V(f_i) \cap V(f_j)|$ is equal to the frequency of $(0,0)^T$ in any i-th, j-th rows of $A(f_1, f_2, \ldots, f_m; \mathbf{W})$. Since $A(f_1, f_2, \ldots, f_m; \mathbf{W})$ is a balanced array, $|V(f_i) \cap V(f_j)|$ in $\mathbf{W}$ must be constant $\mu_{0,0}$. ∎

Therefore a projective group on $\mathbf{PG}(3,q)$ is used to generate varieties systematically as many as possible. Let $V(f)$ be a quadric in $\mathbf{PG}(3,q)$ and $\Gamma = \{\alpha_1 = 1, \alpha_2, \cdots, \alpha_g\}$ be a projective group of order g on $\mathbf{PG}(3,q)$. For any $\alpha_i \in \Gamma$, $V(f_i) = V(f)^{\alpha_i}$ is given by $f_i(\mathbf{x}) = \mathbf{x}^T\mathbf{T}_i^T\mathbf{Q}\mathbf{T}_i\mathbf{x}$ for $1 \leq i \leq g$,

where $f(\mathbf{x}) = \mathbf{x}^T\mathbf{Q}\mathbf{x}$ and $\mathbf{T}_i$ is a matrix representation of α_i. Then g quadrics can be constructed as

$$V(f_1), V(f_2), \ldots, V(f_g) \text{ such that } |V(f_i)| = |V(f_j)|, 1 \leq i, j \leq g.$$

In order to satisfy a condition $|V(f_i) \cap V(f_j)| = \mu_{00}$, $i \neq j$, we define a projective group on $\mathbf{PG}(3, q)$ as follows:

Let $\alpha_{(\pi,P)}$ be a projectivity on $\mathbf{PG}(3, q)$ which fixes a plane π pointwise and a point $P \in \pi$ linewise. There are q such projectivities on $\mathbf{PG}(3, q)$ for given π and P. The set of q projectivities forms a projective group $\Gamma_{(\pi,P)}$ of order q. Moreover, let $\Gamma_{(\pi,l)} = \bigcup_{P \in l} \Gamma_{(\pi,P)}$, where l is a line on π, which is also a projective group of order $q(q+1)-q = q^2$. Then q^2 quadratic functions $G = \{f_1, f_2, \ldots, f_{q^2}\}$ can be constructed by using $\Gamma_{(\pi,l)}$.

In the next section it will be shown that $G = \{f_1, f_2, \ldots, f_{q^2}\}$ is useful to construct a balanced array of strength 2, where $V(f_i)$'s are elliptic or hyperbolic quadrics.

2.4 Main Constructions

The discriminant of a quadratic equation plays a key role in the construction here. To solve the quadratic equation

$$ax^2 + bx + c = 0, \quad a \neq 0 \tag{2.1}$$

over $\mathbf{GF}(q)$ with $q = p^h$, $h \geq 1$, the two cases of odd and even characteristic are separately considered.

(i) Let $p \neq 2$. The discriminant of the equation (2.1) is given by $\Delta =$

$b^2 - 4ac$. The number of solutions of (2.1) is

$$\begin{cases} 1 & \text{if } \Delta = 0, \\ 0 & \text{if } \Delta \text{ is a non-square element of } \mathbf{GF}(q), \\ 2 & \text{if } \Delta \text{ is a square element of } \mathbf{GF}(q). \end{cases}$$

(ii) Let $p = 2$. If $b = 0$, then the equation (2.1) has one solution $x = \sqrt{\frac{c}{a}}$. If $b \neq 0$, let $\delta = ac/b^2$ and $D(t) = t + t^2 + \cdots + t^{2^{h-1}}$. The number of solutions of (2.1) is 0 if $D(\delta) = 1$, and 2 if $D(\delta) = 0$.

The quadratic character χ of $\mathbf{GF}(q)$, 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 $a \neq 0$,

$$\sum_{x \in GF(q)} \chi(x)\chi(x-a) = -1. \tag{2.2}$$

The set $\chi_a = \{(\chi(x), \chi(x-a)) \ ; \ x \in \mathbf{GF}(q)\}$ is considered for an element $a \in \mathbf{GF}(q)$. Let x, y, z, w be the numbers of elements $(1,1)$, $(1,-1)$, $(-1,1)$, $(-1,-1)$, respectively, of χ_a. Then the next two lemmas are obtained.

Lemma 2.1 *For $q \equiv 1$ mod 4, it holds that*

$$\begin{aligned} &x = y = z = \tfrac{q-1}{4}, \quad w = \tfrac{q-5}{4} \quad \textit{if } a \textit{ is a square,} \\ &x = \tfrac{q-5}{4}, \quad y = z = w = \tfrac{q-1}{4} \quad \textit{if } a \textit{ is a non-square.} \end{aligned}$$

Proof. If a is a square, $\chi(-a) = 1$. Each of $(1,0)$ and $(0,1)$ appears exactly once in χ_a. Hence it follows that

$$x+y+1 = \tfrac{q-1}{2}, z+w = \tfrac{q-1}{2}, x+z+1 = \tfrac{q-1}{2},$$
$$y+w = \tfrac{q-1}{2}, x+w+1 = y+z,$$

the last of which is from (2.2). Its unique solution is given by $x = y = z = (q-1)/4$ and $w = (q-5)/4$.

If a is a non-square, $\chi(-a) = -1$. Similarly it follows that

$$x+y = \tfrac{q-1}{2}, z+w+1 = \tfrac{q-1}{2}, x+z = \tfrac{q-1}{2},$$
$$y+w+1 = \tfrac{q-1}{2}, x+w+1 = y+z.$$

Thus there exists an unique solution $x = (q-5)/4$, and $y = z = w = (q-1)/4$.

Lemma 2.2 *For $q \equiv 3$ mod 4, it holds that*

$$x = y = w = \tfrac{q-3}{4}, \quad z = \tfrac{q+1}{4}, \quad \textit{if a is a square}$$
$$x = z = w = \tfrac{q-3}{4}, \quad y = \tfrac{q+1}{4}, \quad \textit{if a is a non-square}$$

Proof. This follows from the same manner as Lemma 2.1. ∎

Moreover the following well-known results over $\mathbf{GF}(q)$ with $q = 2^h$, $h \geq 1$, are obtained (see Hirschfeld, 1979).

Result 2.4 *Let $C_0 = \{t \in \mathbf{GF}(q);\ D(t) = 0\}$ and $C_1 = \{t \in \mathbf{GF}(q);\ D(t) = 1\}$ for $q = 2^h$. Then*

1. $0 \in C_0$,
2. $t \in C_i \Rightarrow t^\sigma \in C_i$ *for any automorphism σ of* $\mathbf{GF}(q)$,
3. $s \in C_i, t \in C_j \Rightarrow s+t \in C_0$ *if* $i = j$, $s+t \in C_1$ *if* $i \neq j$,
4. $|C_0| = |C_1| = q/2$.

Lemma 2.3 *Let* $t = kx/(ax+b)^2$ $(k, a, b \neq 0)$ *for* $x \in \mathbf{GF}(q)$ *with* $q = 2^h$, $h \geq 2$. *Then* $|\{t \in \mathbf{GF}(q)\ ;\ t \in C_1\}|$ *is zero if* $k = ab$ *and* $q/4$ *if* $k \neq ab$.

Proof. Suppose $t \in C_1$. A quadratic equation $ta^2x^2+kx+tb^2 = 0$ on x must have two solutions. Let $\delta = t^2a^2b^2/k^2$. Since $\delta \in C_0$, we have a condition $(ab/k)t \in C_0$. Consider the following two cases.
(I) $k = ab$.
In this case $t \in C_0$ which contradicts the assumption. Hence there is no t such that $t \in C_1$.
(II) $k \neq ab$.
We now consider the intersection of $\{t \in \mathbf{GF}(q)\ ;\ t \in C_1\}$ and $\{t \in \mathbf{GF}(q)\ ;\ (ab/k)t \in C_0\}$. Since $\mathbf{GF}(2^h) \cong \mathbf{GF}(2)^h$, let $S = \{\xi \in \mathbf{GF}(2)^h\ ;\ \xi \in C_0\}$. Then S is a subspace of $\mathbf{GF}(2)^h$ and $|S| = q/2$. Thus S is regarded as a hyperplane of $\mathbf{GF}(2)^h$. That is, the incidence matrix of elements of $\mathbf{GF}(2)^h \setminus \{0\}$ and the hyperplanes shows an Hadamard 2-$(2^h-1, 2^{h-1}-1, 2^{h-2})$ design. Hence $|\{t \in \mathbf{GF}(q)\ ;\ t \in C_1\} \cap \{t \in \mathbf{GF}(q)\ ;\ (ab/k)t \in C_0\}| = 2^{h-2} = q/4$. ■

Recall that a projective group $\Gamma_{(\pi,l)}$ and a set of quadratic forms $G = \{f_1, f_2, \ldots, f_{q^2}\}$ which are defined in Section 2.3. Now the following three cases are considered to construct arrays $A(f_1, f_2, \ldots, f_m; \mathbf{W})$.

Case 1

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

$\mathbf{W}_1 = \pi_1 - l$, where π_1 is a non-fixed tangent plane of $V(f_1)$ by $\Gamma_{(\pi_0,l)}$.

Case 2

G_1 is the same as in Case 1.

$\mathbf{W}_2$ is a coset of $L(\pi_0)$ distinct from $L(\pi_0)$, where $L(\pi_0) = \{t\mathbf{x}\ ;\ t \in \mathbf{GF}(q),\ \mathbf{x} \in \pi_0\}$.

Case 3

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

$\mathbf{W}_2$ is the same as in Case 2.

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

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

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

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

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

where $l = \{(1,0,0,0)^T \cup (t,1,0,0)^T \; ; \; t \in \mathbf{GF}(q)\}$, $\pi_0 = \{(x_0,x_1,x_2,x_3)^T \in \mathbf{PG}(3,q) \; ; \; x_2 = 0 \text{ and } x_0,x_1,x_3 \in \mathbf{GF}(q)\}$. Then the quadratic forms which are constructed by $\Gamma_{(\pi_0,l)}$ is expressed by

(i) $f_i(\mathbf{x}) \in G_1$ for $1 \leq i \leq q^2$; $f_i(\mathbf{x}) = dx_0^2 + x_0x_1 + (b+2ad)x_0x_2 + x_1^2 + (a+2b)x_1x_2 + (ab+b^2+a^2d)x_2^2 + x_2x_3$,

(ii) $f_i(\mathbf{x}) \in G_2$ for $1 \leq i \leq q^2$; $f_i(\mathbf{x}) = x_0x_1 + bx_0x_2 + ax_1x_2 + abx_2^2 + x_2x_3$.

Furthermore, $\mathbf{W}_1$ and $\mathbf{W}_2$ are given by

$$\mathbf{W}_1 = \{\mathbf{x} = (x_0,x_1,x_2,x_3)^T \in \mathbf{GF}(q)^4; x_2 = 1, x_3 = 0 \text{ and } x_0,x_1 \in \mathbf{GF}(q)\},$$

$$\mathbf{W}_2 = \{\mathbf{x} = (x_0,x_1,x_2,x_3)^T \in \mathbf{GF}(q)^4 \; ; \; x_2 = 1 \text{ and } x_0,x_1,x_3 \in \mathbf{GF}(q)\}.$$

When $\mathbf{x}$ extends over the elements of $\mathbf{W}$, $\mathbf{Tx}$ also extends over the elements of $\mathbf{W}$. Hence it follows that the number of solutions to the system of equations for $\mathbf{x}$

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

is equal to the number of solutions to

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

by using linear transformation, where $2 \leq k \leq q^2$ and $1 \leq i, j \leq q^2$, $i \neq j$.

Here it will be shown that Case 1 produces a balanced array of strength 2. For the collection $A(f_1, f_2, \ldots, f_m; \mathbf{W})$, let A^* denotes a juxtaposition of wA for $w \in \mathbf{GF}(q)^*$, where $\mathbf{GF}(q)^* = \mathbf{GF}(q) \setminus \{0\}$. Then A^* is described as $A^*(f_1, f_2, \ldots, f_m; \mathbf{W})$. To show that $A^*(f_1, f_2, \ldots, f_{q^2}; \mathbf{W})$ is a balanced array of strength two, we may count the number of solutions $\mathbf{x}$ for the system of equations

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

depending on values of the parameter $w \in \mathbf{GF}(q)^*$, where $2 \leq k \leq q^2$. This procedure will be taken in the proof of the following theorem.

Theorem 2.4 *Let $\mathbf{W}_1 = \pi_1 - l$ and $f_1, \ldots, f_{q^2}$ be quadratic functions of G_1. Then $A^*(f_1, f_2, \ldots, f_{q^2}; \mathbf{W}_1)$ is a $BA(q^2(q-1), q^2, q, 2)$, for an odd prime*

power q with indices

$$\mu_{\alpha,\beta} = \begin{cases} 0 & \text{if } \alpha = \beta = 0, \\ 1 & \text{if } \alpha \neq 0 \text{ and } \beta = 0, \\ q & \text{if } \alpha = \beta \neq 0, \\ q+1 & \text{if } \alpha \neq \beta \text{ and } \alpha, \beta \neq 0. \end{cases} \tag{2.3}$$

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

$$\bigcup_{w \in \mathbf{GF}(q)^*} \{\mathbf{x} \in \mathbf{W}_1 \,;\, f_1^*(\mathbf{x}) = 0 \text{ and } f_k^*(\mathbf{x}) = 0\}$$

satisfies (2.3) for any α, β, where

$$f_1^*(\mathbf{x}) = dx_0^2 + x_0x_1 + x_1^2 - w\alpha x_2^2 + x_2x_3 = 0, \tag{2.4}$$

$$\begin{aligned} f_k^*(\mathbf{x}) \;=\; & dx_0^2 + x_0x_1 + (b+2ad)x_0x_2 + x_1^2 + (a+2b)x_1x_2 \\ & + (ab + b^2 + a^2d - w\beta)x_2^2 + x_2x_3 = 0. \end{aligned} \tag{2.5}$$

By subtracting (2.4) from (2.5) and taking $x_2 = 1$ and $x_3 = 0$, it holds that

$$(b+2ad)x_0 + (a+2b)x_1 + u + w(\alpha - \beta) = 0, \tag{2.6}$$

where $u = ab + b^2 + a^2d$.
(I) Let us assume that $a + 2b \neq 0$. From (2.4) and (2.6), we obtain the following quadratic equation on x_0:

$$\begin{aligned} & u(1-4d)x_0^2 + a(1-4d)[u + w(\alpha - \beta)]x_0 \\ & \qquad + w\alpha(a+2b)^2 - [u + w(\alpha - \beta)]^2 = 0. \end{aligned} \tag{2.7}$$

The discriminant Δ of (2.7) is given by

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

In order to have a solution of (2.7), Δ must be zero or a square element of $\mathbf{GF}(q)$. That is, $\Delta' = [u+w(\alpha-\beta)]^2 - 4uw\alpha$ should be zero or a non-square. We now consider the number of solutions of (2.7) depending on values of w.

Case 1: $\alpha = \beta = 0$.

Since $\Delta' = u^2$ and $u \neq 0$, (2.7) has no solution.

Case 2: $\alpha = 0$ or$\beta = 0$.

If $\alpha = 0$, then $\Delta' = (u - w\beta)^2$. Hence (2.7) has one solution when $w = u\beta^{-1}$. Similarly, if $\beta = 0$, (2.7) has one solution when $w = u\alpha^{-1}$.

Case 3: $\alpha = \beta \neq 0$.

There are two solutions of (2.7) when the w is one of $(q-1)/2$ 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 $\mathbf{W}_1$.

Case 4: $\alpha \neq \beta$ and $\alpha, \beta \neq 0$.

Without loss of generality we can put $\alpha = 1$, then $\Delta' = (u+w(1-\beta))^2 - 4uw$. Consider a solution w of $(1-\beta)^2w^2 - 2u(1+\beta)w + u^2 - \Delta' = 0$. Then its discriminant $\Delta'' = (1-\beta)^2\Delta' + 4\beta u^2$ must be zero or a square element of $\mathbf{GF}(q)$. If $\Delta' = 0$ and β is a square, then $\Delta'' = 4\beta u^2$ becomes a square. Hence there are two solutions for w.

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

$$n_1 = |\{\Delta' \in \mathbf{GF}(q)^*; \chi(\Delta') = -1 \text{ and } \chi((1-\beta)^2\Delta' + 4\beta u^2) = 0\}|,$$

$$n_2 = |\{\Delta' \in \mathbf{GF}(q)^*; \chi(\Delta') = -1 \text{ and } \chi((1-\beta)^2\Delta' + 4\beta u^2) = 1\}|.$$

In case of $q \equiv 1 \pmod 4$, $n_1 = 1$ if β is a non-square, while $n_1 = 0$ if β is a square. Since $\chi((1-\beta)^2\Delta') = \chi(\Delta')$ for all $\Delta' \in \mathbf{GF}(q)$, by Lemma 2.1, $n_2 = (q-1)/4$. When w is one of $[(q-1)/4] \times 2 + 1 = (q+1)/2$ different values and β is a non-square, (2.7) has two solutions. When w is one of $[(q-1)/4] \times 2$ distinct values and β is a square, (2.7) has also two solutions. Hence there exist $q+1$ solutions in the domain $\mathbf{W}_1$ when β is a non-zero element of $\mathbf{GF}(q)$.

In case of $q \equiv 3 \pmod 4$, $n_1 = 0$ if β is a non-square, while $n_1 = 1$ if β is a square. It follows from Lemma 2.2 that $n_2 = (q+1)/4$ if β is a non-square and $n_2 = (q-3)/4$ if β is a square. When w is one of $(q+1)/4 \times 2 = (q+1)/2$ distinct values and β is a non-square, (2.7) has two solutions. When w is one of $[(q-3)/4] \times 2 + 1 = (q-1)/2$ distinct values and β is a square, (2.7) has two solutions. Thus, in both cases , β is a square or a non-square, we have totally $q+1$ solutions in the domain $\mathbf{W}_1$.

(II) Next, assume that $a + 2b = 0$. The equation (2.6) becomes

$$b(1-4d)x_0 + u + w(\alpha - \beta) = 0, \tag{2.8}$$

which, with (2.4), yields the quadratic equation of x_1 as

$$\begin{aligned} & b^2(1-4d)^2x_1^2 - b(1-4d)(u + w(\alpha-\beta))x_1 \\ & + -w\alpha b^2(1-4d)^2 + d(u + w(\alpha-\beta))^2 = 0. \end{aligned} \tag{2.9}$$

The discriminant Δ of (2.9) is given by

$$\Delta = b^2(1-4d)^3\{[u + w(\alpha-\beta)]^2 - 4uw\alpha\}$$

since $u = ab + b^2 + a^2d = -b^2(1-4d)$. Similarly to the previous four cases on α and β, we can determine the number of solutions of (2.9).

Therefore we complete the proof for any $\alpha, \beta \in \mathbf{GF}(q)$. ∎

Theorem 2.5 *Let* $\mathbf{W}_1 = \pi_1 - l$ *and* $f_1, \ldots, f_{q^2}$ *be quadratic functions of* G_1. *Then* $A^*(f_1, f_2, \ldots, f_{q^2}; \mathbf{W}_1)$ *is a* $BA(q^2(q-1), q^2, q, 2)$, *for an even prime power* q *with indices*

$$\mu_{\alpha,\beta} = \begin{cases} 0 & \text{if } \alpha = \beta = 0, \\ 1 & \text{if } \alpha \neq 0 \text{ and } \beta = 0, \\ q & \text{if } \alpha = \beta \neq 0, \\ q+1 & \text{if } \alpha \neq \beta \text{ and } \alpha, \beta \neq 0. \end{cases} \tag{2.10}$$

Proof. For an even prime power q, a quadratic function of G_1 is given by

$f_k(\mathbf{x}) = dx_0^2 + x_0x_1 + bx_0x_2 + x_1^2 + ax_1x_2 + (ab + b^2 + a^2d)x_2^2 + x_2x_3$.

Similarly to the proof of Theorem 2.4, it can be shown that, the number of elements in

$$\bigcup_{w \in \mathbf{GF}(q)^*} \{\mathbf{x} \in \mathbf{W}_1 \,;\, f_1^*(\mathbf{x}) = 0 \text{ and } f_k^*(\mathbf{x}) = 0\}$$

satisfies (2.10) for any α, β, where

$$f_1^*(\mathbf{x}) = dx_0^2 + x_0x_1 + x_1^2 + w\alpha x_2^2 + x_2x_3 = 0, \tag{2.11}$$

$$\begin{aligned} f_k^*(\mathbf{x}) \;=\; & dx_0^2 + x_0x_1 + bx_0x_2 + x_1^2 + ax_1x_2 \\ & + (ab + b^2 + a^2d + w\beta)x_2^2 + x_2x_3 = 0. \end{aligned} \tag{2.12}$$

By subtracting (2.11) from (2.12) and taking $x_2 = 1$ and $x_3 = 0$, it holds that

$$bx_0 + ax_1 + u + w(\alpha + \beta) = 0, \tag{2.13}$$

where $u = ab + b^2 + a^2d$.

(I) Assume $a \neq 0$. From (2.11) and (2.13), we obtain the quadratic equation of x_0

$$ux_0^2 + a[u + w(\alpha + \beta)]x_0 + w\alpha a^2 + [u + w(\alpha + \beta)]^2 = 0. \qquad (2.14)$$

If $w = u(\alpha+\beta)^{-1}$, (2.14) have one solution for $\alpha \neq \beta$. Let $u+w(\alpha+\beta) \neq 0$. In order to have two solutions of the equation (2.14), the discriminant δ of (2.14) must be an element of C_0 (see Result 2.4), where

$$\delta = \frac{uw\alpha}{(u + w(\alpha + \beta))^2} + \frac{u}{a^2}.$$

By Result 2.4, it can be shown that $u/a^2 = b/a+b^2/a^2+d \in C_1$ and $d \in C_1$. Hence we will find the number of w such that $(uw\alpha)/[u + w(\alpha + \beta)]^2 (= \delta', \text{say}) \in C_1$. By Lemma 2.3, we have

$$|\{w \in \mathbf{GF}(q)^*; \delta' \in C_1\}| = \begin{cases} 0 & \text{if } \alpha = 0 \text{ or } \beta = 0, \\ \frac{q}{2} & \text{if } \alpha, \beta \neq 0. \end{cases}$$

Hence the number of elements in $\bigcup_{w \in \mathbf{GF}(q)^*} \{\mathbf{x} \in \mathbf{W}_1 \,;\, f_1^*(\mathbf{x}) = 0 \text{ and } f_k^*(\mathbf{x}) = 0\}$ is given by

$$\mu_{\alpha,\beta} = \begin{cases} 0 & \text{if } \alpha = \beta = 0, \\ 1 & \text{if } \alpha \neq 0 \text{ and } \beta = 0, \\ q & \text{if } \alpha = \beta \neq 0, \\ q+1 & \text{if } \alpha \neq \beta \text{ and } \alpha, \beta \neq 0. \end{cases}$$

(II) Assume $a = 0$. Then $u = b^2$. From (2.11) and (2.13), we obtain the quadratic equation of x_1 as

$$ux_1^2 + b(u + w(\alpha + \beta))x_1 + w\alpha u + d(u + w(\alpha + \beta))^2 = 0. \qquad (2.15)$$

We can prove the number of solutions by a technique similar to (I).

Therefore $A^*(f_1, f_2, \ldots, f_{q^2}; \mathbf{W}_1)$ is a $BA(q^2(q-1), q^2, q, 2)$ with indices given by (2.10). ■

Next we consider Cases 2 and 3. It will be shown that these constructions give orthogonal arrays. The following result is a generalized case of the theorem of Bézout (see Semple and Roth, 1986).

Result 2.5 *If the intersection of $V(f_1)$ and $V(f_2)$ is a curve C, then the degree of C is $m_1 m_2$, where m_1 and m_2 are the degree of f_1 and f_2, respectively.*

This is useful to derive the next two lemmas.

Lemma 2.4 *Let $\mathbf{W}_2$ be a coset of $L(\pi_0)$ distinct from $L(\pi_0)$, and let $f_1, \ldots, f_{q^2}$ be quadratic functions of G_1. Then $A(f_1, f_2, \ldots, f_{q^2}; \mathbf{W}_2)$ is an $OA(q^3, q^2, q, 2)$ of index q for any prime power q .*

Proof. It will be shown that the number of solutions to the system of equations for $\mathbf{x} \in \mathbf{GF}(q)^4$ as

$$\begin{cases} f_1(\mathbf{x}) &= dx_0^2 + x_0x_1 + x_1^2 + x_2x_3 = \alpha, \\ f_k(\mathbf{x}) &= dx_0^2 + x_0x_1 + (b+2ad)x_0x_2 + x_1^2 \\ & \quad +(a+2b)x_1x_2 + (ab + b^2 + a^2d)x_2^2 + x_2x_3 = \beta. \end{cases} \tag{2.16}$$

is q for any $\alpha, \beta \in \mathbf{GF}(q)$. Since we the domain $\mathbf{W}_2 = \{\mathbf{x} = (x_0, x_1, x_2, x_3)^T \in \mathbf{GF}(q)^4 \; ; \; x_2 = 1\}$ is considered, the number of solutions of (2.16) is the same as that of the system of equations as

$$\begin{cases} f_1^*(\mathbf{x}) &= dx_0^2 + x_0x_1 + x_1^2 - \alpha x_2^2 + x_2x_3 = 0, \\ f_k^*(\mathbf{x}) &= dx_0^2 + x_0x_1 + (b+2ad)x_0x_2 + x_1^2 \\ & \quad +(a+2b)x_1x_2 + (ab + b^2 + a^2d - \beta)x_2^2 + x_2x_3 = 0, \end{cases}$$

for $2 \leq k \leq q^2$. Hence it is sufficient to consider the intersection of elliptic quadrics $V(f_1^*)$ and $V(f_k^*)$ in $\mathbf{PG}(3, q)$. Extend the space $\mathbf{PG}(3, q)$ to

$\mathbf{PG}(3, q^2)$, then $V(f_1^*)$ becomes a hyperbolic quadric in $\mathbf{PG}(3, q^2)$. In the quadratic extension $\mathbf{PG}(3, q^2)$ of $\mathbf{PG}(3, q)$, 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 $V(f_k^*)$. So $V(f_1^*)$ and $V(f_k^*)$ have two lines l_1 and l_2 of $\mathbf{PG}(3, q^2)$ in common.

By Result 2.5, $V(f_1^*)$ and $V(f_k^*)$ intersect in a curve of degree 4. Since the curve of degree 4 contains two lines l_1 and l_2, the remaining part of the intersection in $\mathbf{PG}(3, q^2)$ 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 $V(f_k^*)$ contains no line of $\mathbf{PG}(3, q)$. Therefore, in $\mathbf{PG}(3, q)$, $V(f_1^*)$ meets $V(f_k^*)$ in a conic which consists of q points and the fixed point $l_1 \cap l_2$. Thus the number of solutions of (2.16) is q in $\mathbf{W}_2$ for any $\alpha, \beta \in \mathbf{GF}(q)$. ■

Lemma 2.5 *Let $\mathbf{W}_2$ be a coset of $L(\pi_0)$ distinct from $L(\pi_0)$, and let $f_1, \ldots, f_{q^2}$ be quadratic functions of G_2. Then $A(f_1, f_2, \ldots, f_{q^2}; \mathbf{W}_2)$ is an $OA(q^3, q^2, q, 2)$ of index q for any prime power q.*

Proof. Similarly to Lemma 2.4, it will be shown that the hyperbolic quadrics $V(f_1^*)$ and $V(f_k^*)$ have $3q + 1$ points of $\mathbf{PG}(3, q)$ in common, where

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

Note that $V(f_1^*)$ and $V(f_k^*)$ are hyperbolic quadrics also in the quadratic extension $\mathbf{PG}(3, q^2)$. By using the same argument as the proof of Lemma 2.4, the intersections of $V(f_1^*)$ and $V(f_k^*)$ consist of two lines l_1, l_2 on π_0 and a curve of degree 2 in $\mathbf{PG}(3, q^2)$. If the curve is the union of two lines, then one of them is l_1 or l_2. Hence in both cases, $V(f_1^*)$ meets $V(f_k^*)$ in $3q + 1$ points of $\mathbf{PG}(3, q)$. Therefore the number of solutions in $\mathbf{W}_2$ to the system of equations, $f_1(\mathbf{x}) = \alpha$ and $f_k(\mathbf{x}) = \beta$, for $\mathbf{x}$, is q for any $\alpha, \beta \in \mathbf{GF}(q)$. ■

The OAs given in Lemmas 2.4 and 2.5 do not form linear subspace themselves and their parameters are not new. However, they may be a cosets of a linear subspace.

Now, we consider a domain $\mathbf{W}_3$ on $\mathbf{PG}(3,q^2)$. Let $\bar{\pi}_0 = \{\mathbf{x} \in \mathbf{PG}(3,q^2)\,;\ \mathbf{x} \in \pi_0\}$ and $\bar{L}(\bar{\pi}_0) = \{t\mathbf{x}\,;\ t \in \mathbf{GF}(q^2),\ \mathbf{x} \in \bar{\pi}_0\}$. Then we define $\mathbf{W}_3$ as a coset of $\bar{L}(\bar{\pi}_0)$ distinct from $\bar{L}(\bar{\pi}_0)$. In this case the following two theorems are immediate from Lemmas 2.4 and 2.5.

Theorem 2.6 *Let $\mathbf{W}_2$ be a coset of $L(\pi_0)$ distinct from $L(\pi_0)$, let $\mathbf{W}_3$ be a coset of $\bar{L}(\bar{\pi}_0)$ distinct from $\bar{L}(\bar{\pi}_0)$, and let $f_1, \ldots, f_{q^2}$ be quadratic functions of G_1. Then $A(f_1, f_2, \ldots, f_{q^2}; \mathbf{W}_3 - \mathbf{W}_2)$ is a $BA(q^6 - q^3, q^2, q^2, 2)$, for any prime power q, with indices*

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

Proof. By Lemma 2.4, the number of solutions of (2.16) in $\mathbf{W}_3$ is q^2 for any $\alpha, \beta \in \mathbf{GF}(q^2)$, while the number of solutions of (2.16) in $\mathbf{W}_2$ is q for any $\alpha, \beta \in \mathbf{GF}(q)$. Therefore the number of solutions of (2.16) in $\mathbf{W}_3 - \mathbf{W}_2$ is $q^2 - q$ for any $\alpha, \beta \in \mathbf{GF}(q)$. ∎

Theorem 2.7 *Let $\mathbf{W}_2$ be a coset of $L(\pi_0)$ distinct from $L(\pi_0)$, let $\mathbf{W}_3$ be a coset of $\bar{L}(\bar{\pi}_0)$ distinct from $\bar{L}(\bar{\pi}_0)$, and let $f_1, \ldots, f_{q^2}$ be quadratic functions of G_2. Then $A(f_1, f_2, \ldots, f_{q^2}; \mathbf{W}_3 - \mathbf{W}_2)$ is a $BA(q^6 - q^3, q^2, q^2, 2)$, for any prime power q, with indices*

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

Proof. It follows from an argument similar to Theorem 2.6. ∎

Chapter 3

Mutually M-intersecting Varieties

Let f be a homogeneous polynomial. Then a set of all points $\mathbf{x}$ of $\mathbf{PG}(n,q)$ satisfying $f(\mathbf{x}) = 0$ is called a variety and denoted by $V(f)$. We consider a set of varieties in $\mathbf{PG}(n,q)$, called a set of mutually M-intersecting varieties, such that each variety contains ρ points and the number of points in the intersection of two distinct varieties is contained in a set M. We are interested in finding varieties as many as possible which are mutually M-intersecting. This is not only an interesting geometrical problem but also an important problem with combinatorial applications.

When $M = \{\mu\}$, we can use the varieties to construct combinatorial designs such as (r,λ)-design and arrays like orthogonal, incomplete orthogonal or balanced arrays. When $|M| = 2$, a set of mutually M-intersecting varieties is related to a particular graph called a *strongly regular graph* which is sometimes used in the design of experiments. This chapter is based on Fuji-Hara and Miyamoto (1997b,c).

3.1 Introduction

Let f be a homogeneous polynomial. The set of points $\mathbf{x}$ of $\mathbf{PG}(n,q)$ satisfying $f(\mathbf{x}) = 0$ is called a *variety* and denoted by $V(f)$. Consider a set of varieties $V(f_1)$, $V(f_2)$, $\cdots$, $V(f_g)$ which satisfies the following three conditions:

(i) M is a set of non-negative integers.

(ii) $|V(f_i)| = \rho$ for $1 \leq i \leq g$.

(iii) $|V(f_i) \cap V(f_j)| \in M$ for $1 \leq i, j \leq g$, $i \neq j$.

The set is denoted by $\mathcal{V}(\rho, M)$. In particular, it is denoted by $\mathcal{V}(\rho, \mu)$ when M is a singleton $\{\mu\}$. Note $g = |\mathcal{V}(\rho, M)|$. Of course, $\mathcal{V}(\rho, \mu)$ satisfies a necessary condition for the existence of a balanced array given in Theorem 2.3.

We first find the maximal number of mutually M-intersecting varieties in $\mathcal{V}(\rho, M)$. In case that M consists of greater than or equals to two elements, the problem of finding the maximal number has not been solved. But in case $M = \{\mu\}$, it is not difficult to derive its upper bound. Let $\mathcal{V}$ be a set of all points of $\mathbf{PG}(n,q)$ and $\mathcal{B} = \{B_1, B_2, \cdots, B_g\}$ be a set $\mathcal{V}(\rho, \mu)$, where $B_i = V(f_i)$ for $i = 1, 2, \ldots, g$. Then there exists an incidence structure represented by the $v \times g$ incidence matrix N between $\mathcal{V}$ and $\mathcal{B}$, and a dual structure of it is an (r, λ)-design, where $r = |B_i| = \rho$ and $\lambda = |B_i \cap B_j| = \mu$. Hence $s = rank N^T N = rank N N^T \leq |\mathcal{V}| = v$, i.e. the number of points on $\mathbf{PG}(n,q)$. Thus it is easy to show the following.

Theorem 3.1 *For any prime power q, the maximal number of mutually $\{\mu\}$-intersecting varieties in $\mathcal{V}(\rho, \mu)$ on $\mathbf{PG}(n,q)$ is $(q^{n+1} - 1)/(q - 1)$.*

We present an example, i.e. $\mathcal{V}(q+1, 1)$ in $\mathbf{PG}(2,q)$, which attains the bound. Let $f = x_0^2 + x_1 x_2$. Then $V(f)$ in $\mathbf{PG}(2,q)$ is called a *conic*. The conic consists of $q + 1$ points.

Example 3.1 Let $V(f)$ be a conic in $\mathbf{PG}(2,q)$ and $\Gamma = \{\alpha_1 = 1, \alpha_2, \cdots, \alpha_g\}$ be the Singer automorphism of $\mathbf{PG}(2,q)$, where $g = q^2+q+1$. If $V(f_i) = \{\mathbf{x}\ ;\ f(\alpha_i\mathbf{x}) = 0\}$ for any $\alpha_i \in \Gamma$, $i = 1, 2, \ldots, g$, then a set of conics $V(f_1)$, $V(f_2)$, $\cdots$, $V(f_g)$ forms a $\mathcal{V}(q+1,1)$ consisting q^2+q+1 conics.

Lemmas 2.4 and 2.5 present constructions of orthogonal arrays by using elliptic quadrics or hyperbolic quadrics in $\mathbf{PG}(3,q)$. Recall that two sets of quadratic functions G_1 and G_2 are given by elliptic quadrics and hyperbolic quadrics respectively. Using G_1 and G_2, the next two theorems will be shown.

Theorem 3.2 *There exists a set of q^2 mutually $\{q+1\}$-intersecting varieties, $\mathcal{V}(q^2+1, q+1)$, in $\mathbf{PG}(3,q)$, where q is any prime power.*

Proof. It is sufficient to consider the intersection of elliptic quadrics $V(f_1)$ and $V(f_k)$ in $\mathbf{PG}(3,q)$, where

$$\begin{aligned} f_1(\mathbf{x}) &= dx_0^2 + x_0x_1 + x_1^2 + x_2x_3, \\ f_k(\mathbf{x}) &= dx_0^2 + x_0x_1 + (b+2ad)x_0x_2 + x_1^2 \\ &\quad +(a+2b)x_1x_2 + (ab+b^2+a^2d)x_2^2 + x_2x_3, \end{aligned}$$

for $a, b \in \mathbf{GF}(q)$. Similarly to Lemma 2.4, it can be seen that $V(f_1)$ meets $V(f_k)$ in a conic which consists of q points and one fixed point. Therefore, for any distinct two functions $f_i, f_j \in G_1$, $V(f_i)$ and $V(f_j)$ have $q+1$ points in common. ∎

Theorem 3.3 *When q is any prime power, there exists a set of q^2 mutually $\{3q+1\}$-intersecting varieties, $\mathcal{V}((q+1)^2, 3q+1)$, in $\mathbf{PG}(3,q)$.*

Proof. Consider a set of hyperbolic quadrics $V(f_1), V(f_2), \ldots, V(f_{q^2})$, where $f_i \in G_2$, $1 \le i \le q^2$. In the proof of Lemma 2.5, it is shown that $V(f_1)$ and $V(f_k)$, where

$$\begin{aligned} f_1(\mathbf{x}) &= x_0x_1 + x_2x_3, \\ f_k(\mathbf{x}) &= x_0x_1 + bx_0x_2 + ax_1x_2 + abx_2^2 + x_2x_3, \end{aligned}$$

have $3q+1$ points in common. Hence this completes the proof. ∎

3.2 Hermitian Varieties

An $(n+1) \times (n+1)$ square matrix $H = (h_{ij})$ with elements from $\mathbf{GF}(q^2)$ is called a *Hermitian matrix* if $h_{ij} = h_{ji}^q$ for all i, j. Let $A^{(q)} = (a_{ij}^q)$ for a matrix $A = (a_{ij})$, $a_{ij} \in \mathbf{GF}(q^2)$. A *Hermitian variety* (abbreviated to HV) is defined as $\{\mathbf{x} \in \mathbf{PG}(2, q^2)\,;\, f(\mathbf{x}) = \mathbf{x}^T H \mathbf{x}^{(q)} = 0\}$, where H is a Hermitian matrix. Here we use $V(H)$ instead of $V(f)$ to denote the Hermitian variety. Two Hermitian matrices H and G are said to be *equivalent* if there exists a non-singular matrix P over $\mathbf{GF}(q^2)$ such that $P^T H P^{(q)} = G$. When H is a Hermitian matrix of rank r, $V(H)$ is called a HV of rank r. A HV of rank $n+1$ in $\mathbf{PG}(n, q^2)$ is said to be nondegenerate. The properties of a HV in $\mathbf{PG}(2, q^2)$ have been studied by Bose and Chakravarti (1966) and Kestenband (1981). A HV in $\mathbf{PG}(2, q^2)$ contains q^2+1, q^3+q^2+1 or q^3+1 points, according to its rank 1, 2, or 3, respectively. It is known that any non-singular Hermitian matrix is equivalent to the identity matrix I.

Note that the minimal polynomial $m(x)$ of a matrix H satisfies $m(H) = \mathbf{0}$ and $m'(H) \neq \mathbf{0}$ for any polynomial $m'(x)$ with $deg(m'(x)) < deg(m(x))$. Kestenband (1981) has showed the following classification of $V(H)$ in $\mathbf{PG}(2, q^2)$ with respect to intersections with $V(I)$.

Result 3.1 (Kestenband, 1981) *Let H be a non-singular Hermitian matrix. Let $m(x)$ and $g(x)$ be minimal and characteristic polynomial of H respectively. Then $V(H) \cap V(I)$ contains*

1. *$(q+1)^2$ points, if $m(x) = g(x) = (x-\alpha)(x-\beta)(x-\gamma)$, α, β, γ distinct elements of $\mathbf{GF}(q)$.*

2. *q^2+q+1 points, if $m(x) = g(x) = (x-\alpha)(x-\beta)^2$, α, β, distinct elements of $\mathbf{GF}(q)$.*

3. $q+1$ *collinear points, if* $m(x) = (x-\alpha)(x-\beta)$, α, β, *distinct elements of* $\mathbf{GF}(q)$.

4. q^2+1 *points, if* $m(x) = g(x) = (x-\alpha)p(x)$ *for* $\alpha \in \mathbf{GF}(q)$ *and* $p(x)$ *is irreducible over* $\mathbf{GF}(q)$.

5. q^2+1 *points, if* $m(x) = g(x) = (x-\lambda)^3$, $\lambda \in \mathbf{GF}(q)^*$.

6. *one point, if* $m(x) = (x-\lambda)^2$, $\lambda \in \mathbf{GF}(q)^*$.

7. q^2-q+1 *points, no three of which are collinear, if* $g(x)$ *is irreducible over* $\mathbf{GF}(q^2)$.

In addition to Result 3.1, Kestenband (1980) generated a set $\mathcal{F}$ consisting of q^2+q+1 Hermitian matrices with irreducible characteristic polynomials over $\mathbf{GF}(q)$. Let H' be a Hermitian matrix with irreducible characteristic polynomials $p(x)$ over $\mathbf{GF}(q)$. Since H' satisfies $p(H') = 0$, the polynomials $p'(H')$ over $\mathbf{GF}(q)$ with $deg(p'(H')) < deg(p(H'))$ form a field $\mathbf{GF}(q^3)$. Let H be a primitive root of this field. Then $\mathcal{F}$ is defined by

$$\mathcal{F} = \{H^i \,;\, 0 \le i \le q^2+q\}.$$

Result 3.2 (Kestenband, 1980) Any two Hermitian varieties $V(H^k)$ and $V(H^l)$ intersect on q^2-q+1 points, where H^k and H^l are from $\mathcal{F}$, $k \neq l$.

The set of varieties derivable from Hermitian matrices in $\mathcal{F}$ directly forms $\mathcal{V}(q^3+1, q^2-q+1)$. Since the set is isomorphic to $\mathbf{PG}(2,q)$, the incidence matrix of the varieties $\mathcal{V}(q^3+1, q^2-q+1)$ and the points on $\mathbf{PG}(2,q^2)$ consists of q^2-q+1 copies of $\mathbf{PG}(2,q)$.

Next a Hermitian matrix with minimal polynomial $(x-1)^3$ is used to construct new mutually M-intersecting varieties which are different from Result 3.2 of Kestenband. We assume in the rest of this section that q is an even prime power. A matrix U is said to be *unitary* if $U^T U^{(q)} = I$. Consider

the following unitary matrix U and group $\mathcal{U}$ of order $q+1$ over $\mathbf{GF}(q^2)$ as

$$U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha^2 \end{pmatrix}, \quad \mathcal{U} = \{I, U, U^2, \ldots, U^q\},$$

where $\alpha^{q+1} = 1$, $\alpha \neq 1$ over $\mathbf{GF}(q^2)$. Let H be a non-singular Hermitian matrix with minimal polynomial $m(x) = (x-1)^3$. Without loss of generality we can put

$$H = \begin{pmatrix} 1 & a & 0 \\ a^q & 1 & b \\ 0 & b^q & 1 \end{pmatrix}, \quad a^{q+1} + b^{q+1} = 0,$$

where $a, b \in \mathbf{GF}(q^2) \setminus \{0\}$. Using the unitary group $\mathcal{U}$, a set of HV's is defined by $\mathcal{H} = \{V(H_1), V(H_2), \ldots, V(H_{q+1})\}$ with $H_i = U^{iT} H U^{i(q)}$ and $U^i \in \mathcal{U}$. Then H_i is expressed by

$$H_i = \begin{pmatrix} 1 & a\alpha^{iq} & 0 \\ a^q\alpha^i & 1 & b\alpha^{iq} \\ 0 & b^q\alpha^i & 1 \end{pmatrix}.$$

Note that any $V(H_i) \in \mathcal{H}$ is a nondegenerate HV which contains q^3+1 points.

Theorem 3.4 *Let q be an even prime power. Then $\mathcal{H}$ is a set of mutually M-intersecting varieties, $\mathcal{V}(q^3+1, q^2+1)$, where $|\mathcal{V}(q^3+1, q^2+1)| = q+1$.*

Proof. It will be shown that any distinct two HV's $V(H_i)$ and $V(H_j)$ of $\mathcal{H}$ have q^2+1 points in common. It follows that $|V(H_i) \cap V(H_j)| = |V(U^{iT} H U^{i(q)}) \cap V(U^{jT} H U^{j(q)})| = |V(U^{i+kT} H U^{i+k(q)}) \cap V(H)|$ for some k such that $U^{j+k} = I_3$. Hence we only show that the number of points of $V(H_i) \cap V(H)$ for any $V(H_i) \in \mathcal{H}$, $H_i \neq H$, is q^2+1. Moreover we have $|V(H_i) \cap V(H)| = |V(P^T H_i P^{(q)}) \cap V(I)|$, where P is a non-singular matrix

such that $P^t H P^{(q)} = I$:

$$P = \begin{pmatrix} 1 & a^q t & a^q b^q t \\ 0 & t & b^q t^q \\ 0 & 0 & t^{-1} \end{pmatrix},$$

where $t^{q+1}(a^{q+1}+1) = 1$ over $\mathbf{GF}(q^2)$. The characteristic polynomial of $P^T H_i P^{(q)}$ is $\det(P^T H_i P^{(q)} - xI) = \det(P^T H_i P^{(q)} - xP^t H P^{(q)}) = \det(P^T)$ $\det(H_i - xH_j)\det(P^{(q)}) = \det(H_i - xH_j) = (x-1)^3$. When the first row of $P^T H_i P^{(q)}$ is expressed by $\mathbf{p}^T = (1, at^q(1+\alpha^i)^q, abt(1+\alpha^i)^q)$, the (1,1)-entry of $(P^t H_i P^{(q)} - I)^2$ is $\mathbf{p}^T\mathbf{p}^{(q)} + 1 = 1 + a^{q+1}t^{q+1}(1+\alpha^i)^{q+1} + a^{q+1}b^{q+1}t^{q+1}(1+$ $\alpha^i)^{q+1} + 1 = a^{q+1}(1+\alpha^i)^{q+1} \neq 0$ by using $t^{q+1}(1+b^{q+1}) = 1$. Since $(P^T H_i P^{(q)} - I)^2 \neq \mathbf{0}$, the minimal polynomial of $P^T H_j P^{(q)}$ is $(x-1)^3$. Hence we have $|V(H_i) \cap V(H)| = q^2 + 1$ from Result 3.1. ∎

Next consider two non-singular Hermitian matrices H and H' both having the minimal polynomial $m(x) = (x-1)^3$. Then as mentioned before Theorem 3.4, two sets can be defined as follows:

$$\mathcal{H}_{a,b} = \{V(H_1), V(H_2), \ldots, V(H_{q+1})\} \text{ with } H_i = {U^i}^T H U^{i(q)} \text{ and } U^i \in \mathcal{U},$$

$$\mathcal{H}_{c,d} = \{V(H'_1), V(H'_2), \ldots, V(H'_{q+1})\} \text{ with } H'_j = {U^j}^T H' U^{j(q)} \text{ and } U^j \in \mathcal{U},$$

where

$$H = \begin{pmatrix} 1 & a & 0 \\ a^q & 1 & b \\ 0 & b^q & 1 \end{pmatrix}, \qquad H' = \begin{pmatrix} 1 & c & 0 \\ c^q & 1 & d \\ 0 & d^q & 1 \end{pmatrix},$$

$a^{q+1} + b^{q+1} = 0, \quad c^{q+1} + d^{q+1} = 0, \quad a, b, c, d \in \mathbf{GF}(q^2) \setminus \{0\}$,
In order to obtain $\mathcal{H}_{a,b}$ and $\mathcal{H}_{c,d}$ which are disjoint, we have to restrict a,b,c, and d. Let w be a primitive element of the multiplicative group $\mathbf{GF}(q^2) \setminus \{0\}$ of order $q^2 - 1$. Let $K = \{1, w^{q-1}, \ldots, w^{q(q-1)}\}$ be a multiplicative subgroup of order $q+1$ and $K_k = K \cdot w^k$ for k cosets of K, $0 \leq k \leq q-2$. Suppose

$a \in K_l$, $0 \leq l \leq q-2$. Then the (2,2)-entry $a\alpha^{iq}$ of H_i, $1 \leq i \leq q+1$, is also an element of K_l since α is included in K. Hence for $1 \leq i \leq q+1$, $a\alpha^{iq}$ extends over all the elements of K_l. Since $a^{q+1} + b^{q+1} = 0$, $b \in K_l$. Hence we have to choose c and d from cosets K_k, $k \neq l$, to satisfy $\mathcal{H}_{a,b} \cap \mathcal{H}_{c,d} = \phi$.

Theorem 3.5 *Let q be an even prime power. If a and c belong to different cosets K_k and K_l respectively, then $\mathcal{H}_{a,b} \cup \mathcal{H}_{c,d}$ is a set of mutually M-intersecting varieties, $\mathcal{V}(q^3+1, M)$, where $M \subseteq \{q^2+1, (q+1)^2\}$ and $|\mathcal{V}(q^3+1, M)| = 2(q+1)$.*

Proof. It follows from Theorem 3.4 that $\mathcal{H}_{a,b}$ and $\mathcal{H}_{c,d}$ are both $\mathcal{V}(q^3+1, q^2+1)$. Now consider the number of points in the intersection of $V(H_i)$ and $V(H'_j)$ for $H_i \in \mathcal{H}_{a,b}$ and $H'_j \in \mathcal{H}_{c,d}$. It is easily seen that $|V(H_i) \cap V(H'_j)| = |V(H) \cap V(H'_{j+k})|$ for some k such that $U^{i+k} = I_3$. Furthermore, we have $|V(H) \cap V(H'_j)| = |V(I_3) \cap V(P^T H'_j P^{(q)})|$, where P is a non-singular matrix such that $P^T H P^{(q)} = I$. The characteristic polynomial $g(x)$ of $P^T H'_j P^{(q)}$ is $(x-1)(x^2+\delta x+1)$, where $\delta = (ac^q + bd^q)\alpha^{qi} + (a^q c + b^q d)\alpha^i$. The quadratic equation $x^2+\delta x+1 = 0$ has one solution over $\mathbf{GF}(q)$ if $\delta = 0$. Then we have $g(x) = (x-1)^3$ and $(P^t H_j P^{(q)} - xI)^2 \neq \mathbf{0}$. Hence the minimal polynomial $m(x)$ of $P^T H'_j P^{(q)}$ is $m(x) = (x-1)^3$. When the equation $x^2 + \delta x + 1 = 0$ has two solutions, $m(x) = g(x) = (x-1)(x-\beta)(x-\gamma)$, where $\beta, \gamma \in \mathbf{GF}(q)$ such that $\beta \neq \gamma$, $\beta \neq 1$ and $\gamma \neq 1$. When the equation has no solutions, $m(x) = g(x) = (x-1)(x^2+\delta x+1)$; that is, $x^2+\delta x+1$ is irreducible over $\mathbf{GF}(q)$. Therefore $V(P^T H'_j P^{(q)})$ and $V(I)$ intersect on q^2+1 or $(q+1)^2$ points. ∎

In the proof of Theorem 3.5, if $\delta = 0$, the minimal polynomial $m(x)$ of $P^T H'_j P^{(q)}$ is $(x-1)^3$. When $a = b$ and $c = d$, we always obtain $\delta = 0$. Since $|V(H) \cap V(H'_j)| = q^2+1$ for $H_i \in \mathcal{H}_{a,b}$ and $H'_j \in \mathcal{H}_{c,d}$, the following can be obtained.

Corollary 3.1 *Let q be an even prime power. If $a = b$ and $c = d$, then $\mathcal{H}_{a,b} \cup \mathcal{H}_{c,d}$ is a set of $2(q+1)$ mutually M-intersecting varieties, $\mathcal{V}(q^3+1, q^2+1)$.*

Finally we want to get a set of Hermitian varieties $\mathcal{H}_{a,b}$ as many as possible by choosing the values of a and b in H.

Theorem 3.6 *Let q be an even prime power. There exists a set of q^2-1 mutually M-intersecting varieties, $\mathcal{V}(q^3+1, q^2+1)$.*

Proof. Let $J = \{1, w, \ldots, w^{q-2}\}$ be a set of representatives of the cosets $K_k = K \cdot w^k$, $0 \leq k \leq q-2$. Consider a set of varieties $\bigcup_{a \in J} \mathcal{H}_{a,a}$. If we choose $a, c \in J$, $a \neq c$, then $\mathcal{H}_{a,a} \cup \mathcal{H}_{c,c}$ is $\mathcal{V}(q^3+1, q^2+1)$ by Corollary 3.1. Hence $\bigcup_{a \in J} \mathcal{H}_{a,a}$ is $\mathcal{V}(q^3+1, q^2+1)$ consisting of $(q+1)(q-1)$ varieties. ■

Theorem 3.7 *Let q be an even prime power. There exists a set of $(q+1)^2(q-1)$ mutually M-intersecting varieties $\mathcal{V}(q^3+1, \{q^2+1, (q+1)^2\})$.*

Proof. Let $J = \{1, w, \ldots, w^{q-2}\}$ be a set of representatives of the cosets K_k. Let $L = \{(a,b)\,;\, a^{q+1} + b^{q+1} = 0, a \in J, b \in \mathbf{GF}(q^2)\}$. Then L consists of $(q-1)(q+1)$ elements and $\mathcal{H}_{a,b} \cap \mathcal{H}_{c,d} = \phi$ for $(a,b), (c,d) \in L$, $(a,b) \neq (c,d)$. Therefore Theorem 3.5 implies that $\bigcup_{(a,b) \in L} \mathcal{H}_{a,b}$ is $\mathcal{V}(q^3+1, \{q^2+1, (q+1)^2\})$. ■

We remark that we can add $V(I)$ to $\mathcal{V}(\rho, M)$ in all the theorems given in this section because we can show $|V(H_i) \cap V(I)| = q^2+1$ for any $V(H_i) \in \mathcal{H}$.

Chapter 4

Conclusion

Since Chakravarti introduced balanced arrays in 1956, many methods of constructions have been investigated. Some of them depend on the existence of block designs with proper parameters. However, some of such methods do not give algebraic constructions which are used for orthogonal arrays. This is a reason why we have studied an algebraic method for constructing balanced arrays. First, we generalized the construction of orthogonal arrays which was proposed by Bose in 1947. In the generalization, we used multivariate functions instead of linear transformations and a subset of $\mathbf{GF}(q)^n$ instead of $\mathbf{GF}(q)^n$ itself as their domain. Secondly, we utilized two kinds of quadratic functions on a projective geometry as multivariate functions in Chapter 2. In the application of the present method, we found a necessary condition for the existence of balanced arrays. It was deeply related to a set of points called a variety on projective geometry. We generated a set of varieties satisfying the necessary condition by using a projective group to construct balanced arrays. Thirdly, we proposed an interesting mathematical problem to find a set of varieties such that each variety contains ρ points and the number of points in the intersection of two distinct varieties, called mutually M-intersecting varieties, is contained in a set M. When M consists of a singleton, a set of mutually M-intersecting varieties is very useful to construct

balanced arrays. In Chapter 3, we showed constructions of some sets of mutually M-intersecting varieties by using Hermitian forms on a projective plane, however, s-symbols balanced arrays have not been obtained yet.

Lastly, we give a list of balanced arrays and a set of mutually M-intersecting varieties obtained in this thesis.

- $BA(q^2(q-1), q^2, q, 2)$ for any odd prime power q with indices

$$\mu_{\alpha,\beta} = \begin{cases} 0 & \text{if } \alpha = \beta = 0, \\ 1 & \text{if } \alpha \neq 0 \text{ and } \beta = 0, \\ q & \text{if } \alpha = \beta \neq 0, \\ q+1 & \text{if } \alpha \neq \beta \text{ and } \alpha, \beta \neq 0. \end{cases} \quad \text{(Theorem 2.4).}$$

- $BA(q^2(q-1), q^2, q, 2)$ for any $q = 2^h$, $h \geq 1$, with indices

$$\mu_{\alpha,\beta} = \begin{cases} 0 & \text{if } \alpha = \beta = 0, \\ 1 & \text{if } \alpha \neq 0 \text{ and } \beta = 0, \\ q & \text{if } \alpha = \beta \neq 0, \\ q+1 & \text{if } \alpha \neq \beta \text{ and } \alpha, \beta \neq 0. \end{cases} \quad \text{(Theorem 2.5).}$$

- $OA(q^3, q^2, q, 2)$ for any prime power q with index $\mu = q$ (Lemmas 2.4 and 2.5).

- $BA(q^6 - q^3, q^2, q^2, 2)$ for any prime power q with indices

$$\mu_{\alpha,\beta} = \begin{cases} q^2 - q & \text{if } \alpha, \beta \in \mathbf{GF}(q), \\ q^2 & \text{if otherwise,} \end{cases} \quad \text{(Theorems 2.6 and 2.7)}$$

For any prime power q,

- $\mathcal{V}(q^2+1, q+1)$ in $\mathbf{PG}(3, q)$, where $|\mathcal{V}| = q^2$, (Theorem 3.2).

- $\mathcal{V}((q+1)^2, 3q+1)$ in $\mathbf{PG}(3, q)$, where $|\mathcal{V}| = q^2$ (Theorem 3.3).

For any $q = 2^h$, $h \geq 1$,

- $\mathcal{V}(q^3+1, q^2+1)$ in $\mathbf{PG}(2, q^2)$, where $|\mathcal{V}| = q+1$ (Theorem 3.4).
- $\mathcal{V}(q^3+1, M)$ in $\mathbf{PG}(2, q^2)$, where $M \subseteq \{q^2+1, (q+1)^2\}$ and $|\mathcal{V}| = 2(q+1)$ (Theorem 3.5).
- $\mathcal{V}(q^3+1, q^2+1)$ in $\mathbf{PG}(2, q^2)$, where $|\mathcal{V}| = 2(q+1)$ (Corollary 3.1).
- $\mathcal{V}(q^3+1, q^2+1)$ in $\mathbf{PG}(2, q^2)$, where $|\mathcal{V}| = q^2-1$ (Theorem 3.6).
- $\mathcal{V}(q^3+1, \{q^2+1, (q+1)^2\})$ in $\mathbf{PG}(2, q^2)$, where $|\mathcal{V}| = (q+1)^2(q-1)$ (Theorem 3.7).

Bibliography

Addelman, S. and Kempthorne, O. (1961). Some main-effect plans and orthogonal arrays of strength two. *Ann. Math. Statist.*, 32:1167–1176.

Beth, T., Jungnickel, D. and Lenz, H. (1985). *Design Theory.* Bibliographisches Instit, Zurich.

Bose, R. C. (1947). Mathematical theory of the symmetrical factorial design. *Sankhyā*, 8:107–166.

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

Bose, R. C. and Chakravarti, I. M. (1966). Hermitian varieties in a finite projectice space $PG(N, q^2)$. *Can. J. Math.*, 17:1161–1182.

Bose, R. C., Shrikhande, S. S. and Parker, E. (1960). Further results on the construction of mutually orthogonal latin squares and the falsity of euler's conjecture. *Can. J. Math.*, 12:189–203.

Bose, R. C. and Srivastava, J. N. (1964a). Analysis of irregular factorial fractions. *Sankhyā* (A), 26:117–144.

Bose, R. C. and Srivastava, J. N. (1964b). Multidimensional partially balanced designs and their analysis with applications to partially balanced factorial fractions. *Sankhyā* (A), 26:145–168.

Box, G. E. P. and Hunter, J. S. (1961). The 2^{k-p} fractional factorial designs, Part I, II. *Technometrics*, 3:311–351.

Bush, K. A. (1952a). A generalization of a theorem due to MacNeish. *Ann. Math. Statist.*, 23:293–295.

Bush, K. A. (1952b). Orthogonal arrays of index unity. *Ann. Math. Statist.*, 23:426–434.

Chakravarti, I. M. (1956). Fractional replication in asymmetrical factorial designs and partially balanced arrays. *Sankhyā*, 17:143–164.

Chakravarti, I. M. (1961). On some methods of construction of partially balanced arrays. *Ann. Math. Statist.*, 32:1181–1185.

Chakravarti, I. M. and Dey, A. (1976). On the construction of balanced and orthogonal arrays. *Canad. J. Statist.*, 4:109–117.

Chopra, D. V. (1975a). Balanced optimal 2^8 fractional factorial designs of resolution V, $52 \leq N \leq 59$. In *A Survey of Statistical Design and Linear Models*, 91–99.

Chopra, D. V. (1975b). Optimal balanced 2^8 fractional factorial designs of resolution V with 60 to 65 runs. *Proc. Internat. Statist. Inst.*, 46:161–166.

Chopra, D. V. (1977a). Some optimal balanced reduced designs of resolution V for 2^9 series. *Proc. Internat. Statist. Inst.*, 47:120–123.

Chopra, D. V. (1977b). Trace-optimal balanced 2^9 reduced designs of resolution V with 46 to 54 runs. *J. Indian Statist. Assoc.*, 15:179–186.

Chopra, D. V. (1979). Balanced optimal resolution V designs for ten bi-level factors, $57 \leq N \leq 65$. *Proc. Internat. Statist. Inst.*, 48:103–105.

Chopra, D. V. (1982). A note on balanced arrays of strength four. *Sankhyā* (B), 44:71–75.

Chopra, D. V. (1983a). Factorial designs for 2^{10} series and simple arrays. *Proc. Internat. Statist. Inst.*, 50:854–857.

Chopra, D. V. (1983b). A note on an upper bound for the constraints of balanced arrays with strength t. *Commun. Statist.-Theor. Meth.*, 12:1755–1759.

Chopra, D. V. (1985). On balanced arrays with two symbols. *Ars Combinatoria.*, 20:59–63.

Chopra, D. V. (1990). Further combinatorial investigations on balanced arrays. *Ars Combinatoria*, 29C:27–32.

Chopra, D. V. (1991). Further investigations on balanced arrays. *Comput. Statist. & Data Analysis*, 12:231–237.

Chopra, D. V. (1995). On arrays with some combinatorial structure. *Discrete Math.*, 138:193–198.

Chopra, D. V., Kipngeno, W. A. K. and Ghosh, S. (1986). More precise tables of optimal balanced 2^m fractional factorial designs of Srivastava and Chopra, $7 \leq m \leq 10$. *J. Statist. Plann. Inference*, 25:115–121.

Chopra, D. V. and Srivastava, J. N. (1973a). Optimal balanced 2^7 fractional factorial designs of resolution V, with $N \leq 42$. *Ann. Inst. Statist. Math.*, 25:587–604.

Chopra, D. V. and Srivastava, J. N. (1973b). Optimal balanced 2^7 fractional factorial designs of resolution V, $49 \leq N \leq 55$. *Commun. Statist.*, 2:59–84.

Chopra, D. V. and Srivastava, J. N. (1974). Optimal balanced 2^8 fractional factorial designs of resolution V, $37 \leq N \leq 51$. *Sankhyā* (A), 36:41–52.

Chopra, D. V. and Srivastava, J. N. (1975). Optimal balanced 2^7 fractional factorial designs of resolution V, $43 \leq N \leq 48$. *Sankhyā* (B), 37:429–447.

Dey, A., Kulshreshtha, A. C. and Saha, G. M. (1972). Three symbol partially balanced arrays. *Ann. Inst. Statist. Math.*, 24:525–528.

Euler, L. (1782). Recherches sur une nouvelle espéce des quarrés magiques. *Verhandlingen Zeeuwach Genootschap Wetenschappen Vlissengen*, 9:85–239. See also (Euler, 1923).

Euler, L. (1923). Recherches sur une nouvelle espéce des quarrés magiques. *Leonardi Eulei Opera Omnia*, 7:291–392.

Finney, D. J. (1945). The fractional replication of factorial arrangements. *Ann. Eugen.*, 12:291–301.

Fisher, R. A. (1926). The arrangement of field experiments. *J. Ministry of Agriculture*, 33:503–513.

Fisher, R. A. (1942). The theory of confounding in factorial experiments in relation to the theory of groups. *Ann. Eugen.*, 11:341–353.

Fuji-Hara, R., Jimbo, M. and Yuan, F. (1989). A recursive construction of balanced arrays. *Utilitas Math.*, 36:83–92.

Fuji-Hara, R. and Kuriki, S. (1991). Mutually balanced nested designs. *Discrete Math.*, 97:167–176.

Fuji-Hara, R., Kuriki, S. and Jimbo, M. (1989). On balanced complementation for regular t-wise balanced designs. *Discrete Math*, 76:29–35.

Fuji-Hara, R., Kuriki, S. and Miyake, M. (1996). Cyclic orthogonal and balanced arrays. *J. Statist. Plann. Inference*, 56:171–180.

Fuji-Hara, R. and Miyamoto, N. (1995). Balanced arrays from quadratic functions. submitted to J. Statist. Plann. Inference.

Fuji-Hara, R. and Miyamoto, N. (1997a). A construction of combinatorial arrays from non-linear functions. submitted to J. Combin. Designs.

Fuji-Hara, R. and Miyamoto, N. (1997b). Mutually M-intersecting Hermitian varieties. submitted to Finite Field and Their Applications.

Fuji-Hara, R. and Miyamoto, N. (1997c). Mutually M-intersecting varieties. *Congressus Numerantium.* to appear.

Hall, M. (1986). *Combinatorial Theory.* Second Edition, John Wiley & Sons.

Hirschfeld, J. (1979). *Projective Geomotries over Finite Fields.* Oxford University Press, New York.

Hirschfeld, J. (1985). *Finite Projective Spaces of ThreeDimenseions.* Oxford University Press, New York.

Hirschfeld, J. and Thas, J. (1991). *General Galois Geometries.* Oxford University Press, New York.

Horton, J. (1974). Sub-latin squares and incomplete orthogonal arrays. *J. Combin. Theory* (A), 16:23–33.

Hughes, D. and Piper, F. (1973). *Projective Planes.* Springer-Verlag, New York.

Hyodo, Y. (1992). Characteristic-polynomials of information matrices of some balanced fractional 2^m factorial designs of resolution $2l + 1$. *J. Statist. Plann. Inference*, 31:245–252.

Hyodo, Y. (1994). Characterization of information matrices for balanced two-level fractional factorial designs of odd resolution derived from two-symbol simple arrays. *Commun. Statist.-Theor. Meth.*, 23:1859–1874.

Hyodo, Y. and Kuwada, M. (1994). Analysis of variance of balanced fractional s^m factorial designs of resolution $V_{p,q}$. *J. Statist. Plann. Inference*, 23:263–277.

James, A. T. (1957). The relationship algebra of an experimental design. *Ann. Math. Statist.*, 28:993–1002.

Kageyama, S. (1975). Note on the construction of partially balanced arrays. *Ann. Inst. Statist. Math.*, 27:177–180.

Kestenband, B. (1980). Projective geometries that are disjoint unions of caps. *Can. J. Math.*, 32(6):1299–1305.

Kestenband, B. (1981). Unital intersections in finite projective planes. *Geometriae Dedicata*, 11:107–117.

Kiefer, J. (1959). Optimum experimental designs. *J. Roy. Statist. Soc.* (B), 21:272–319.

Kuriki, S. (1984a). Existence conditions for balanced arrays of strength t, $t+2$ constraints and s symbols. *TRU Math.*, 20:139–161.

Kuriki, S. (1984b). General existence condition for balanced arrays of strength t, m constraints and s symbols. *TRU Math.*, 20:191–211.

Kuriki, S. (1988). Existence of 2-symbol balanced arrays of strength-t and $t+2$ constraints. *J. Statist. Plann. Inference*, 20:225–228.

Kuriki, S. (1993). On existence and construction of balanced arrays. *Discrete Math.*, 116:137–155.

Kuriki, S. and Fuji-Hara, R. (1994). Balanced arrays of strength two and nested (r, λ)-designs. *J. Combin. Designs*, 2:407–414.

Kuriki, S. and Yamamoto, S. (1984). Nonsimple 2-symbol balanced arrays of strength t and $t+2$ constraints. *TRU Math.*, 20:249–263.

Kuwada, M. (1979a). Balanced arrays of strength 4 and balanced fractional 3^m factorial designs. *J. Statist. Plann. Inference*, 3:347–360.

Kuwada, M. (1979b). Optimal balanced fractional 3^m factorial designs of resolution V and balanced third-order designs. *Hiroshima Math. J.*, 9:347–450.

Kuwada, M. (1981). Characteristic polynomials of the information matrices of balanced fractional 3^m factorial designs of resolution V. *J. Statist. Plann. Inference*, 5:189–209.

Kuwada, M. (1986). Balanced fractional 2^{m_1} factorial designs of resolution V for interesting effects orthogonal to some effects concerning m_2 factors. *J. Statist. Plann. Inference*, 13:365–376.

Kuwada, M. (1988). A-optimal partially balanced fractional $2^{m_1+m_2}$ factorial designs of resolution V, with $4 \leq m_1 + m_2 \leq 6$. *J. Statist. Plann. Inference*, 18:177–193.

Kuwada, M. (1993). Robustness of balanced fractional 2^m factorial designs derived from simple arrays. *Discrete Math.*, 116:183–208.

Kuwada, M. and Kuriki, S. (1986). Some existence conditions for partially balanced arrays with 2 symbols. *Discrete Math.*, 61:221–233.

Kuwada, M. and Nishii, R. (1979). On a connection between balanced arrays and balanced fractional s^m factorial designs. *J. Japan Statist. Soc.*, 9:93–101.

Kuwada, M. and Nishii, R. (1988). On the characteristic polynomial of the information matrix of balanced fractional s^m factorial designs of resolution $V_{p,q}$. *J. Statist. Plann. Inference*, 18:101–114.

Margolin, B. H. (1969). Resolution IV fractional factorial designs. *J. Roy. Statist. Soc.* (B), 31:514–523.

Nishii, R. (1981). Balanced fractional $r^m \times s^n$ factorial designs and their analysis. *Hiroshima Math. J.*, 11:379–413.

Nishii, R. and Shirakura, T. (1986). More precise tables of Srivastava-Chopra balanced optimal 2^m fractional factorial designs of resolution V, $m \leq 6$. *J. Statist. Plann. Inference*, 13:111–116.

Ohnishi, T. and Shirakura, T. (1985). Search designs for 2^m factorial experiments. *J. Statist. Plann. Inference*, 11:241–245.

Plackett, R. L. and Burman, J. P. (1946). The design of optimum multifactorial experiments. *Biometrika*, 3:305–325.

Rafter, J. A. and Seiden, E. (1974). Contributions to the theory and construction of balanced arrays. *Ann. Statist.*, 2:1256–1273.

Raghavarao, D. (1971). *Constructions and Combinatorial Problems in Design of Experiments.* Wiley, New York.

Rao, C. R. (1946). Hypercubes of strength '*d*' leading to confounded designs in factorial experiments. *Bull. Calcutta Math. Soc.*, 38:67–78.

Rao, C. R. (1947). Factorial experiments derivable from combinatorial arrangements of arrays. *J. Roy. Statist. Soc. Suppl.*, 9:128–139.

Rao, C. R. (1950). The theory of fractional replication in factorial experiments. *Sankhyā*, 10:81–86.

Saha, G. M., Mukerjee, R. and Kageyama, S. (1988). Bounds on the number of constraints for balanced arrays of strength t. *J. Statist. Plann. Inference*, 18:255–265.

Saha, G. M. and Samanta, B. K. (1985). A construction of balanced arrays of strength t and some related incomplete block designs. *Ann. Inst. Statist. Math.*, 37(2):337–345.

Seiden, E. (1954). On the problem of construction of orthogonal arrays. *Ann. Math. Statist.*, 25:151–156.

Seiden, E. and Zemach, R. (1966). On orthogonal arrays. *Ann. Math. Statist.*, 37:1355–1370.

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

Shirakura, T. (1975). On balanced of 2 symbols, strength $2l$, m constraints and index set $\{\mu_0, \mu_1, \ldots, \mu_{2l}\}$ with $\mu_l = 0$. *J. Japan Statist. Soc.*, 5:53–56.

Shirakura, T. (1976a). Balanced fractional 2^m factorial designs of even resolution obtained from balanced array of strength $2l$ with index $\mu_l = 0$. *Ann. Statist.*, 4:723–735.

Shirakura, T. (1976b). Optimal balanced fractional 2^m factorial designs of resolution VII, $6 \leq m \leq 8$. *Ann. Statist.*, 4:515–531.

Shirakura, T. (1977). Contributions to balanced fractional 2^m factorial designs derived from balanced arrays of strength $2l$. *Hiroshima Math. J.*, 7:217–285.

Shirakura, T. (1980). Necessary and sufficient condition for a balanced array of strength $2l$ to be a balanced fractional 2^m factorial design of resolution $2l$. *Austral. J. Statist.*, 22:69–74.

Shirakura, T. and Kuwada, M. (1975). Note on balanced fractional 2^m factorial designs of resolution $2l+1$. *Ann. Inst. Statist. Math.*, 27:377–386.

Shirakura, T. and Kuwada, M. (1976). Covariance matrices of the estimates for balanced fractional 2^m factorial designs of resolution $2l+1$. *J. Japan Statist. Soc.*, 6:27–31.

Shirakura, T. and Ohnishi, T. (1985). Search designs for 2^m factorial derived from balanced arrays of strength $2(l+1)$ and AD-optimal search designs. *J. Statist. Plann. Inference*, 11(2):247–258.

Shirakura, T. and Ohnishi, T. (1992). A series of search designs for 2^m factorial designs of resolution V which permit search of one or two unknown extra three-factor interactions. *Ann. Inst. Statist. Math.*, 44:185–196.

Shirakura, T. and Ohnishi, T. (1996). Weighted A-optimality for fractional 2^m factorial designs of resolution V. *J. Statist. Plann. Inference*, 56(2):243–256.

Shrikhande, S. S. and Bhagwandas (1969). On embedding of orthogonal arrays of strength two. In *Combinatorial Mathematics and Its Application*, 256–273. Univ. of North Carolina.

Srivastava, J. N. (1970). Optimal balanced 2^m fractional factorial designs. *S.N. Roy Memorial Volume, Univ. of North Carolina and Indian Statist. Institute*, 689–706.

Srivastava, J. N. (1972). Some general existence conditions for balanced arrays of strength t and 2 symbols. *J. Combinatorial Theory* (A), 13:198–206.

Srivastava, J. N. and Anderson, D. A. (1970). Some basic properties of multidimensional partially balanced designs. *Ann. Math. Statist.*, 41:1438–1445.

Srivastava, J. N. and Anderson, D. A. (1971). Fractional association schemes with applications to the construction of multidimensional partially balanced designs. *Ann. Math. Statist.*, 42:1167–1181.

Srivastava, J. N. and Bose, R. C. (1966). Some economic partially balanced 2^m factorial fractions. *Ann. Inst. Statist. Math.*, 18:57–73.

Srivastava, J. N. and Chopra, D. V. (1971a). Balanced optimal 2^m fractional factorial designs of resolution V, $m \leq 6$. *Technometrics*, 13:257–269.

Srivastava, J. N. and Chopra, D. V. (1971b). On the characteristic roots of the information matrix of 2^m balanced factorial designs of resolution V, with applications. *Ann. Math. Statist.*, 42:722–734.

Srivastava, J. N. and Chopra, D. V. (1973). Balanced arrays and orthogonal arrays. In Srivastava, J. N. et al., editor, *A Survey of Combinatorial Theory*, 411–428. North-Holland publishing company.

Srivastava, J. N. and Chopra, D. V. (1974). Balanced trace-optimal 2^7 fractional factorial designs of resolution V, with 56 to 68 runs. *Utilitas Math.*, 5:263–279.

Srivastava, J. N. and Ghosh, S. (1976). A series of balanced 2^m factorial designs of resolution V which allow search and estimation of one extra unknown effect. *Sankhyā* (B), 38:280–289.

Srivastava, J. N. and Ghosh, S. (1977). Balanced 2^m factorial designs of resolution V which allow search and estimation of one extra unknown effect, $4 \leq m \leq 8$. *Commun. Statist.-Theor. Meth.*, 6:141–166.

Srivastava, J. N. and Wijetunga, A. M. (1981). Balanced arrays of strength t with three symbols and $(t + 1)$ rows. *Jr. Comb., Inf. & Syst. Sci.*, 6:335–355.

Street, A. P. and Street, D. J. (1987). *Combinatorics of Experimental Design.* Oxford University Press.

Takahashi, I. (1979). *Combinatorial Theory and The Applications (in Japanese).* Iwanami Shoten, Tokyo.

Yamamoto, S., Kuriki, S. and Natori, S. (1984). Some nonsimple 2-symbol balanced arrays of strength t and $t+2$ constraints. *TRU Math.*, 20:225–228.

Yamamoto, S., Kuriki, S. and Yuan, F. (1983). Balanced arrays of strength t, $t+1$ constraints and s symbols. *TRU Math.*, 19:105–114.

Yamamoto, S., Kuwada, M. and Yuan, F. (1985). On the maximum number of constraints for s-symbol balanced arrays of strength t. *Commun. Statist.-Theor. Meth.*, 14:2447–2456.

Yamamoto, S., Shirakura, T. and Kuwada, M. (1975). Balanced arrays of strength $2l$ and balanced fractional 2^m factorial designs. *Ann. Inst. Statist. Math.*, 27:143–157.

Yamamoto, S., Shirakura, T. and Kuwada, M. (1976). Characteristic polynomials of the information matrices of balanced fractional 2^m factorial designs of higher $(2l+1)$ resolution. In Ikeda, S. et al., editor *Essays in Probability and Statistics*, Shinko Tsusho, Tokyo, 73–94.

Yates, F. (1937). The design and analysis of factorial experiments. *Imperial Bureau of Soil Science, Technical Communications*, 35.

Yuan, F. (1992). Characterization of singular balanced fractional s^m factorial designs derivable from balanced arrays with maximum number of constraints. *Commun. Statist.-Theor. Meth.*, 21:1891–1907.

Yuan, F., Jimbo, M. and Fuji-Hara, R. (1991). An extension method for balanced arrays. *Commun. Statist.-Theor. Meth.*, 20:1073–1085.