CHAPTER 3

Balanced Arrays

3.1. Introduction

For the convenience of the reader, we restate the definition of a balanced array. Let S be a set $\{0, 1, \cdots, s-1\}$ of s *elements* and let S^t be the set of all t-dimensional column vectors with elements from S. A *balanced array* of *strength* t, denoted by $\mathrm{BA}(v, b, s, t)$, is an $v \times b$ matrix $\boldsymbol{A}$ with entries from S satisfying the following conditions:

(A1): in any two-rowed submatrix $\boldsymbol{A}_0$ of $\boldsymbol{A}$, any t-vector $\boldsymbol{x} \in S^t$ occurs exactly $\mu(\boldsymbol{x})$ times as columns in $\boldsymbol{A}_0$, and

(A2): for any permutation σ of order t and for any $\boldsymbol{x} \in S^t$, $\mu(\boldsymbol{x}) = \mu(\sigma(\boldsymbol{x}))$.

The $\mu(\boldsymbol{x})$'s are called the *indices*, and v the number of *constraints*.

As mentioned in Section 1.3, many people have contributed to the development of the theory of balanced arrays. Research in this field are classified into two branches: one is to find the existence conditions and the other is to find actual methods of construction.

It is known that balanced arrays of v constraints cannot exist for all set of values of parameters. Necessary and sufficient conditions for the existence of 2-symbol balanced arrays of strength t were obtained for $v = t + 1$ and $t + 2$ by Srivastava [Sri72] and for $v = t + 3$ by Shirakura [Shi77]. Srivastava [Sri72] also gave some necessary conditions in terms of systems of Diophantine equations, and Srivastava and Chopra [SC73] investigated these necessary conditions extensively. For

3-symbol balanced arrays, Srivastava and Wijetunga [**SW81**] established a necessary and sufficient condition for the existence of balanced arrays with $t+1$ constraints. Their results, however, involved several errors to be corrected. Necessary and sufficient conditions for the existence of an s-symbol balanced array have been obtained for $v = t+1$ by Yamamoto, Kuriki and Yuan [**YKY83**], who also corrected Lemma 7.1 of Srivastava and Wijetunga [**SW81**], and for $v \geq t+2$ by Kuriki [**Kur84a, Kur84b, Kur88**]. For upper bounds on the maximum number of constraints for balanced arrays, the interested reader is referred to Chopra [**Cho82, Cho83**], Rafter and Seiden [**RS74**], Saha, Mukerjee and Kageyama [**SMK88**], and Yamamoto, Kuwada and Yuan [**YKY85**].

Many balanced arrays have been constructed from other combinatorial structures. In fact, block designs are closely related to balanced arrays. The incidence matrices of a BIBD and an (r, λ)-design are balanced arrays with appropriate parameters. Chakravarti [**Cha61**], Rafter and Seiden [**RS74**], Chakravarti and Dey [**CD76**], and Dey, Kulshreshtha and Saha [**DKS72**] gave a method of constructing 3-symbol balanced arrays of strength two or three from BIBDs. Kageyama [**Kag75**] constructed s-symbol balanced arrays of strength t by generalizing the methods of Dey, Kulshreshtha and Saha [**DKS72**]. Kuriki and Fuji-Hara [**KFH94**] showed a connection between certain (r, λ)-designs having a nested structure and balanced arrays with strength two. Fuji-Hara, Jimbo and Yuan [**FHJY89**] presented a recursive construction for balanced arrays. A cyclic construction by means of cyclic codes was given by Fuji-Hara, Kuriki and Miyake [**FHKM96**]. Fuji-Hara et al. [**FHKK$^+$**] generalized the concept of a nested design introduced in [**KFH94**] and [**FHK91**], and described some construction methods for the generalized nested designs, which in turn can be used to construct balanced arrays.

In the master's thesis [**Shi96**] of the present author, an equivalence relation was established between a balanced array of strength t and a set of algebraic curves which have some properties on intersection points with a 'base' curve. When the genus of the base curve is greater than 0, the relationship holds under the assumption that there exists a set of curves satisfying certain conditions. The existence of such a set of curves was not discussed in that thesis. Fuji-Hara and Shinohara [FHS99] defined and constructed a set of curves whose existence is equivalent to that of a balanced array of strength 2. Such a set of curves is called a *symmetric set of curves*, whose construction will be described in the next two sections.

3.2. Symmetric sets of curves

Let K be a field and C_0 be a curve defined by an equation $F(\boldsymbol{x}) = 0$. If $F \in K[\boldsymbol{x}]$, then C_0 is said to be *defined over* K and denoted by C_0/K. Let $I_P(C, C_0)$ be the intersection multiplicity of C_0 with a curve C at a point P. Also let V be a finite set of points on C_0 and $\mathcal{C}$ a finite set of curves.

Definition 3.2.1. A *symmetric set of curves* is a triple $(C_0, V, \mathcal{C})$ which satisfies the following two conditions:

- for any point $P \in V$, the number of curves C of $\mathcal{C}$ having intersection multiplicity $I_P(C, C_0) = \alpha$ is exactly λ_α, and
- for any ordered pair (P, Q) of distinct points of V, the number of curves $C \in \mathcal{C}$ satisfying $I_P(C, C_0) = \alpha$ and $I_Q(C, C_0) = \beta$ is equal to $\lambda_{\alpha,\beta}$.

Note that $\lambda_{\alpha,\beta} = \lambda_{\beta,\alpha}$ from the definition. We call C_0 the *base curve* of the symmetric set of curves $(C_0, V, \mathcal{C})$.

By comparing the definitions of a balanced array with a symmetric set of curves, it is easily seen that the following theorem holds.

Theorem 3.2.2. *Let C_0 be a curve defined over a finite field. Let $V = \{P_1, \cdots, P_v\}$ and $\mathcal{C} = \{C_1, \cdots, C_b\}$. If $(C_0, V, \mathcal{C})$ is a symmetric* *set of curves, then the $v \times b$ array (n_{ij}) is a balanced array of strength 2, where $n_{ij} = I_{P_j}(C_0, C_i)$.*

In this section, we show a general construction of symmetric sets of curves by using Riemann-Roch Theorem. Throughout this section we suppose that C_0 is defined over $\mathbb{F}_q$ and D is an $\mathbb{F}_q$-rational divisor. Let $L^*(D) = L(D) \setminus \{0\}$.

Theorem 3.2.3. *Let C_0 be a non-singular curve with genus $g = 0$. Let D be an effective divisor on C_0 and F be a curve such that $\mathrm{div}(F) \geq D$. Let $\mathcal{C} = \{f \cdot F : f \in L^*(D)\}$. If $V = \bigcup(\mathrm{Supp}\ (\mathrm{div}(f)) \setminus \mathrm{Supp}\ (\mathrm{div}(F))$ for any $f \in L^*(D)$, then $(C_0, V, \mathcal{C})$ is a symmetric set of curves.*

Proof. For any $f \in L(D)$, $f \cdot F$ is a curve since

$$\mathrm{div}(f \cdot F) = \mathrm{div}(f) + \mathrm{div}(F) = \mathrm{div}(f) + D + \mathrm{div}(F) - D \geq 0.$$

Suppose $\mathrm{div}(f) = \alpha P + \beta Q + E$ for any two distinct points $P, Q \in V$ such that $P, Q \notin \mathrm{Supp}\ E$. Then we have

$$\mathrm{div}(f \cdot F) = \mathrm{div}(f) + \mathrm{div}(F) = \alpha P + \beta Q + E'\ ,\ P, Q \notin \mathrm{Supp}\ E',$$

since $P, Q \notin \mathrm{Supp}\ (\mathrm{div}(F))$. Therefore the intersection multiplicity $I_P(f \cdot F)$ is equal to the order $\mathrm{ord}_P(f)$. Moreover we have

$$|\{f \cdot F : I_P(f \cdot F, C_0) = \alpha, f \in L^*(D)\}| = |\{f \in L^*(D) : \mathrm{ord}_P(f) = \alpha\}|$$

and

$$\begin{aligned} & |\{f \cdot F : I_P(f \cdot F, C_0) = \alpha, I_Q(f \cdot F, C_0) = \beta, f \in L^*(D)\}| \\ = \ & |\{f \in L^*(D) : \mathrm{ord}_P(f) = \alpha, \mathrm{ord}_Q(f) = \beta\}|. \end{aligned}$$

Let $D_P(\alpha) = D - \alpha P$ and $D_{Q,R}(\alpha, \beta) = D - (\alpha Q + \beta R)$, where $P, Q, R \in V$. We can easily see that

$$|\{f \in L^*(D) : \mathrm{ord}_P(f) = \alpha\}| = |L(D_P(\alpha))| - |L(D_P(\alpha + 1))| \quad (3.2.1)$$

and

$$
\begin{aligned}
&|\{f \in L^*(D) : \mathrm{ord}_P(f) = \alpha, \mathrm{ord}_Q(f) = \beta\}| \qquad (3.2.2)\\
= \ &|L(D_{P,Q}(\alpha,\beta))| - |L(D_{P,Q}(\alpha+1,\beta))| - |L(D_{P,Q}(\alpha,\beta+1))|\\
&+|L(D_{P,Q}(\alpha+1,\beta+1))|.
\end{aligned}
$$

When the genus $g = 0$, we can evaluate the dimension of $L(D_{P,Q}(\alpha,\beta))$ from Riemann-Roch Theorem for any pair (P,Q) of distinct points and any pair (α,β) of integers. Since the cardinalities (3.2.1) and (3.2.2) are independent of points P,Q chosen, $(C_0, V, \mathcal{C})$ is a symmetric set of curves. □

Next we consider the case when the genus $g \geq 1$. For a divisor D with $0 \leq \deg D \leq 2g-2$, the dimension of $L(D)$ cannot be obtained from Riemann-Roch Theorem.

Let $M(P,Q;\alpha,\beta) = \{f \in L(D) : \mathrm{ord}_P(f) = \alpha, \mathrm{ord}_Q(f) = \beta\}$. In the same way as the proof of Theorem 3.2.3, we can say that if $M(P,Q;\alpha,\beta) = M(P',Q';\alpha,\beta)$ for any distinct pairs (P,Q) and (P',Q') then $(C_0,V,\mathcal{C})$ is a symmetric set of curves. $M(P,Q;\alpha,\beta)$ is said to be *independent of points* if the cardinality of $M(P,Q;\alpha,\beta)$ is a constant value $\lambda_{\alpha,\beta}$ for any pair (P,Q) of distinct points of V.

Theorem 3.2.4. *Let C_0 be a non-singular curve with genus $g \geq 1$, let D be an effective divisor on C_0 and F a curve such that* $\mathrm{div}(F) \geq D$. *Let $\mathcal{C} = \{f \cdot F : f \in L^*(D)\}$. Suppose $V = \bigcup(\mathrm{Supp}\ (\mathrm{div}(f)) \setminus \mathrm{Supp}\ (\mathrm{div}(F))$ for any $f \in L^*(D)$. If $M(P,Q;\alpha,\beta)$ is independent of points for any pair (α,β), then $(C_0,V,\mathcal{C})$ is a symmetric set of curves.*

In order to apply Theorem 3.2.4, we need to check whether the set $M(P,Q;\alpha,\beta)$ is independent of points for any pair (α,β). In fact, this process can be simplified as the following corollary shows.

Corollary 3.2.5. *If $M(P, Q; \alpha, \beta)$ is independent of points for (α, β) satisfying* $\deg D - 2g + 2 \le \alpha + \beta \le \deg D$*, then (C_0, V, C) is a symmetric set of curves.*

Proof. Let $D_{P,Q}(\alpha, \beta) = D - (\alpha P + \beta Q)$. If $\deg D - 2g + 2 \le \alpha + \beta \le \deg D$, then $0 \le \deg D_{P,Q}(\alpha, \beta) \le 2g - 2$ and the dimension of $L(D_{P,Q}(\alpha, \beta))$ can not be obtained from Riemann-Roch Theorem. Let $N(\alpha, \beta) = \{(\alpha', \beta') : \alpha' \ge \alpha, \beta' \ge \beta, \alpha' + \beta' < \deg D\}$. The cardinality of $L(D_{P,Q}(\alpha, \beta))$ is

$$|L(D_{P,Q}(\alpha, \beta))| = 1 + \sum_{(\alpha', \beta') \in N(\alpha, \beta)} |M(P, Q; \alpha', \beta')|.$$

If $M(P, Q; \alpha', \beta')$ is independent of points for any (α', β') such that $\deg D - 2g + 2 \le \alpha' + \beta' \le \deg D$, then $|L(D_{P,Q}(\alpha, \beta))|$ is also independent of points P and Q chosen. Hence, from (3.2.2) in the proof of Theorem 3.2.3, we can conclude that $M(P, Q; \alpha, \beta)$ is independent of points for any pair (α, β). □

Let C_0 be a curve defined by an equation $f(x, y) = 0$, and let $P = (x_0, y_0)$ be a non-singular point on C_0 such that $\frac{\partial f}{\partial y}(P) \ne 0$. Suppose that the following power series

$$\begin{cases} x = x_0 + t, \\ y = y_0 + h(t), \end{cases} \tag{3.2.3}$$

where

$$h(t) = \sum_{i=1}^{\infty} y_i t^i,$$

satisfy the equation $f(x, y) = 0$. Let C be a curve defined by an equation $c(x, y) = 0$. The intersection multiplicity $I_P(C, C_0)$ at P of curves C_0 with C is the integer l such that

$$c(x_0 + t, y_0 + h(t)) = \alpha t^l + \sum_{i \ge l+1} \alpha_i t^i \ , \ \alpha \ne 0.$$

In general, when the genus $g \geq 1$, it is not easy to find a point set V and a curve set C satisfying the necessary condition of Theorem 3.2.4 or Corollary 3.2.5. We next consider the case $g = 1$, say C_0 is an elliptic curve.

3.3. A construction on an elliptic curve

Let q be a power of prime $p \neq 2$. Suppose, in this section, that $\mathbb{F}_q$ is a finite field of order q and F_{q^m} is an extension of $\mathbb{F}_q$. Let E be a non-singular elliptic curve defined over $\mathbb{F}_q$ given by the polynomial

$$F(x, y) = x^3 + a_2x^2 + a_4x + a_6 - y^2. \tag{3.3.1}$$

We denote an elliptic curve defined over $\mathbb{F}_q$ by $E/\mathbb{F}_q$ and its point at infinity by $\mathcal{O}$.

Theorem 3.3.1. *Let C be the set of all curves defined by quadratic equations over $\mathbb{F}_{q^m}$. Let V be the set of all $\mathbb{F}_{q^m}$-rational intersection points of E with a curve E' which excludes the point $\mathcal{O}$ and P such that $\frac{\partial F}{\partial y}(P) = 0$. If E' is a curve defined by the equation*

$$9x^4 + 12a_2x^3 + (4a_2^2 + 6a_4)x^2 + 4a_2a_4x + a_4^2 - 4(a_2 + 3x)y^2 = 0, \tag{3.3.2}$$

where a_2, a_4 and a_6 are coefficients of the polynomial (3.3.1), then (E, V, C) is a symmetric set of curves.

Proof. Let R be a point not in the set of intersections of E with E'. Let $D = 6r$ and F_0 be a curve with $\mathrm{div}(F_0) = D$. Then the set C of quadratic curves is $C = \{f \cdot F_0 : f \in L^*(D)\}$. We will show that $M(P, Q; \alpha, \beta)$ is independent of points $P, Q \in V$ for any pair (α, β) satisfying $\alpha + \beta = 6$.

Let C be a quadratic curve defined by $G(x, y) = g_1x^2 + g_2y^2 + g_3xy + g_4x + g_5y + g_6 = 0$. By substituting (3.2.3) for x and y of G, we have

$$G(x_0+t, y_0+h(t)) = \mathbf{g}A\mathbf{t}, \tag{3.3.3}$$

where $\mathbf{g} = (g_1, g_2, g_3, g_4, g_5, g_6)$, $\mathbf{t}^T = (1, t, t^2, t^3, t^4, t^5)$ and

$$A^T = \begin{pmatrix} x_0^2 & y_0^2 & x_0y_0 & x_0 & y_0 & 1 \\ 2x_0 & 2y_0y_1 & y_0+x_0y_1 & 1 & y_1 & 0 \\ 1 & y_1^2+2y_0y_2 & y_1+x_0y_2 & 0 & y_2 & 0 \\ 0 & 2y_1y_2+2y_0y_3 & y_2+x_0y_3 & 0 & y_3 & 0 \\ 0 & y_2^2+2y_1y_3+2y_0y_4 & y_3+x_0y_4 & 0 & y_4 & 0 \\ 0 & 2y_2y_3+2y_1y_4+2y_0y_5 & y_4+x_0y_5 & 0 & y_5 & 0 \end{pmatrix}.$$

(B^T is the transpose of the matrix B.) Let $C(P,Q;\alpha,\beta) = \{C \in \mathcal{C} : I_P(C,E) \geq \alpha, I_Q(C,E) \geq \beta\}$. Then $C(P,Q;\alpha,\beta)$ is a linear space of curves. Let $A(P;\alpha)$ be the submatrix of the first α columns of A^T in (3.3.3). Then $\dim C(P,Q;\alpha,\beta)$ is the dimension of the null space of $\mathbf{g}[A(P;\alpha), A(Q;\beta)] = \mathbf{0}$. If $\det A(P;6)$ is equal to 0 then $\dim C(P,Q;6,0) = 1$ since the dimension is 0 or 1. Suppose now that the coefficients y_2 of (3.2.3) corresponding to both P and Q are 0. Then $\dim C(P,Q;6,0) = \dim C(P,Q;0,6) = 1$ since

$$\det A(P;6) = y_2(-2y_3^3 + 3y_2y_3y_4 - y_2^2y_5).$$

Furthermore we have $\dim C(P,Q;3,3) = 1$ because the determinant of the matrix $[A(P;3), A(Q;3)]$ is 0. From Lemma 2.5.3, $C(P,Q;\alpha,\beta) = \{0\}$ for any pair (α,β) satisfying $\alpha+\beta \geq 7$. From Theorem 2.6.4, $\dim C(P,Q;\alpha,\beta) = 1$ for $\alpha+\beta = 5$. Since $\dim C(P,Q;\alpha,\beta) = \dim C(P,Q;\alpha+1,\beta) + \dim C(P,Q;\alpha,\beta+1) - \dim C(P,Q;\alpha+1,\beta+1)$, we have

$$\dim C(P,Q;6,0) = \dim C(P,Q;3,3) = \dim C(P,Q;0,6) = 1$$

and

$$\begin{aligned}\dim C(P,Q;5,1) &= \dim C(P,Q;4,2)\\ &= \dim C(P,Q;2,4) = \dim C(P,Q;1,5) = 0.\end{aligned}$$

Hence, $M(P,Q;\alpha,\beta)$ is independent of points for any pair (α,β) satisfying $\alpha+\beta=6$.

The elliptic curve E is given by

$$F(x,y) = x^3 + a_2x^2 + a_4x + a_6 - y^2 = 0.$$

From $F(x_0+t, y_0+h(t)) = 0$, we have

$$\begin{aligned}&(a_6 + a_4x_0 + a_2x_0^2 + x_0^3 - y_0^2) + (a_4 + 2a_2x_0 + 3x_0^2 - 2y_0y_1)t\\ &+ (a_2 + 3x_0 - y_1^2)t^2 + (1 - 2y_0y_3)t^3 + (-2y_1y_3 - 2y_0y_4)t^4\\ &+ (-2y_1y_4 - 2y_0y_5)t^5 + (-y_3^2 - 2y_1y_5 - 2y_0y_6)t^6 + \cdots\\ &= 0.\end{aligned}$$

Since all coefficients of powers of t must be equal to 0, we have

$$\begin{cases} a_4 + 2a_2x_0 + 3x_0^2 - 2y_0y_1 &= 0\\ a_2 + 3x_0 - y_1^2 &= 0\end{cases}$$

which is equivalent to the equation (3.3.2). Therefore the point (x_0, y_0) is on the curve E' defined by the equation (3.3.2). $\square$

Here we provide an example to illustrate Theorem 3.3.1. Let E be the elliptic curve defined over F_5 given by

$$y^2 = x^3 + x^2 + 2x + 1.$$

Then points $(0,1)$, $(0,4)$, $(3,\omega)$ and $(3,4\omega)$, where ω is a root of x^2+2 in F_{5^2}, are the intersection points of E with the curve given by

$$4x^4+2x^3+x^2+3x+4+y+3xy^2=0.$$

Let V be the set of these four points and $\mathcal{C}$ be the set of quadratic curves defined over F_{5^2}. The power series corresponding to each point of V are

$$\begin{cases} x &= t \\ y &= 1+t+3t^3+3t^4+3t^5+\cdots, \end{cases}$$

$$\begin{cases} x &= t \\ y &= 1+t+3t^3+3t^4+3t^5+\cdots, \end{cases}$$

$$\begin{cases} x &= 3+t \\ y &= \omega+\omega t^3+3\omega t^6+\cdots, \end{cases}$$

$$\begin{cases} x &= 3+t \\ y &= 4\omega+4\omega t^3+2\omega t^6+\cdots. \end{cases}$$

Let $\mathcal{C}(P,Q;\alpha,\beta)=\{C\in\mathcal{C}: I_P(C,E)\geq\alpha, I_Q(C,E)\geq\beta\}$. We see that

$$\dim\mathcal{C}(P,Q;6,0)=\dim\mathcal{C}(P,Q;3,3)=\dim\mathcal{C}(P,Q;0,6)=1$$

and

$$\begin{aligned}\dim\mathcal{C}(P,Q;5,1)&=\dim\mathcal{C}(P,Q;4,2)\\ &=\dim\mathcal{C}(P,Q;2,4)=\dim\mathcal{C}(P,Q;1,5)=0\end{aligned}$$

for any pair (P,Q) of points of V. Hence $(C_0,V,\mathcal{C})$ is a symmetric set of curves with $\lambda_{6,0}=\lambda_{3,3}=\lambda_{0,6}=24$ and $\lambda_{5,1}=\lambda_{4,2}=\lambda_{2,4}=\lambda_{1,5}=0$, where $|\mathcal{C}|=(5^2)^6$.