No. 760

Symmetric Sets of Curves and Combinatorial Arrays

by

Ryoh Fuji-Hara and Satoshi Shinohara

October 1997

Symmetric Sets of Curves and Combinatorial Arrays

Ryoh Fuji-Hara and Satoshi Shinohara

ABSTRACT. Let V be an algebraic curve. $\mathcal{P}$ is a set of points on V. $\mathcal{C}$ is a set of curves each of which intersects V at some points of $\mathcal{P}$. We denote $I_P(C,V)$ as the intersection multiplicity of $C \in \mathcal{C}$ with V at the point $P \in \mathcal{P}$. If $(V,\mathcal{P},\mathcal{C})$ satisfies the following conditions, we call it a *symmetric set of curves*:
(1) for any point $p \in \mathcal{P}$, the number of $\mathcal{C}$ having intersection multiplicity a is λ_a,
(2) for any ordered pair (p,q) points of $\mathcal{P}$, the number of curves $C \in \mathcal{C}$ is equal to $\lambda_{a,b}$ satisfying $I_p(C,V) = a$ and $I_q(C,V) = b$.

When we arrange the multiplicities in an array of size $|\mathcal{C}| \times |\mathcal{P}|$, we have a combinatorial array called a *balanced array*.

We show a general construction of a symmetric set of curves using the Riemann-Roch theorem. We also consider a case that V is an elliptic curve and $\mathcal{C}$ is a set of conics. We show, in this case, the problem is reduced to find a set $\mathcal{P}$ of points which is the intersection of V and a curve of degree 4 derived from V.

1. Introduction

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

DEFINITION 1.1. A *symmetric set of curves* is a triple $(V,\mathcal{P},\mathcal{C})$ which satisfies the following two conditions:

- for any point $p \in \mathcal{P}$, the number of curves of $\mathcal{C}$ having intersection multiplicity a is exactly λ_a, and
- for any ordered pair (p,q) of distinct points of $\mathcal{P}$, the number of curves $C \in \mathcal{C}$ satisfying $I_p(C,V) = a$ and $I_q(C,V) = b$ is equal to $\lambda_{a,b}$.

Note that $\lambda_{a,b} = \lambda_{b,a}$. We call V the *base curve*.

Let $\mathcal{P} = \{p_1, \cdots, p_n\}$ and $\mathcal{C} = \{C_1, \cdots, C_m\}$. If $(V,\mathcal{P},\mathcal{C})$ is a symmetric set of curves, an combinatorial $m \times n$ array $[a_{ij}]$, $a_{ij} = I_{p_j}(V,C_i)$ is called a *balanced array* [1, 2, 4, 8]. A Balanced array may be called a *partial* or *generalized orthogonal array*. An *orthogonal array* is a balanced array with $\lambda_{a,b} = \lambda$.

To construct a symmetric set of curves, we apply a vector space of rational functions over a finite field. We suppose in this paper that the base curve V is defined over a finite field.

1991 *Mathematics Subject Classification.* 05B99,11G20,11G05.

Notations and definitions in this paper are due to [5, 6]. Let F_q be the finite field of order q and $\bar{F}_q$ the algebraic closure of F_q. A point whose coordinates lie in F_q is called a F_q-*rational* point. A *divisor* D on a curve V is a formal sum of $\bar{F}_q$-rational points

$$D = \sum_{p \in V} n_p p,$$

where $n_p \in \mathbf{Z}$ and $n_p = 0$ for all but finitely many $p \in V$. The addition of two divisors is $\sum n_p p + \sum m_p p = \sum (n_p + m_p)p$. The support of D, denoted by Supp D, is the set of points with $n_p \neq 0$. If $n_p \geq 0$ for all $p \in V$ then the divisor is said to be *effective*. The *degree* of D is the integer $\deg D = \sum n_p$.

Let $F \in F_q[x]$ and suppose V is defined by an equation $F(x) = 0$. The *function field* $F_q(V)$ of V over F_q is the field of fractions of the integral domain $F_q[x]/(F)$, where (F) denotes the ideal in $F_q[x]$ generated by F. Similarly, $\bar{F}_q(V)$ is the field of fraction of $\bar{F}_q[x]/(F)$. The elements of $\bar{F}_q(V)$ are called *rational functions.* A non-zero rational function f is said to be *defined at* a point $p \in V$ if there exists a representation $f = g/h, g, h \in \bar{F}_q(V)$ such that $h(p) \neq 0$. If f is not defined at p then we write $f(p) = \infty$. For any $f \in \bar{F}_q(V)$ and $p \in V$, f can be written by $f = u^d s$, where $u, s \in \bar{F}_q(V)$ such that $u(p) = 0$ and $s(p) \neq 0, \infty$. The integer d is said to be the *order of* f *at* p, and denoted by $\mathrm{ord}_p(f)$. The divisor $\mathrm{div}(f)$ of a rational function f is $\sum_p \mathrm{ord}_p(f) \cdot p$.

Let $\mathrm{Aut}(\bar{F}_q/F_q)$ be the Galois group of $\bar{F}_q$ over F_q. We define $p^\sigma = (\sigma(a_0) : \sigma(a_1) : \cdots : \sigma(a_n))$ and $D^\sigma = \sum n_p \sigma(p)$, where $\sigma \in \mathrm{Aut}(\bar{F}_q/F_q)$ and $p = (a_0 : a_1 : \cdots : a_n)$. If a divisor $D = n_1 p_1 + \cdots n_s p_s$ satisfies: (1) there exists a finite extension F_{q^m} such that each p_i is a F_{q^m}-rational point, and (2) $D^\sigma = D$ for any $\sigma \in \mathrm{Aut}(\bar{F}_q/F_q)$, then it is called a *rational divisor over* F_q.

Let $F_q(V)$ be the function field of V over F_q and $L(D) = \{f \in F_q(V) : \mathrm{div}(f) + D \geq 0 \text{ or } f \equiv 0\}$. If D is a rational divisor over F_q then $L(D)$ is a vector space over F_q. The next result is well-known.

RESULT 1.2. If $\deg D < 0$ then $L(D) = \{0\}$.

From the Riemann-Roch theorem, we have the following result.

RESULT 1.3. Let V be a curve of the genus g defined over a finite field F_q. Let D be a rational divisor over F_q on a curve V. If $\deg D > 2g - 2$ then $l(D) = \deg D + 1 - g$, where $l(D)$ is the dimension of $L(D)$.

In the next section, we show a general construction of symmetric sets of curves using the Riemann-Roch theorem.

2. Symmetric sets of curves

We suppose in this section that V is defined over a finite field and D is a rational divisor over a finite field. Let $L(D)^* = L(D) \setminus \{0\}$.

THEOREM 2.1. *Let V be a non-singular curve with the genus $g = 0$. Let D be an effective divisor on V and F a curve such that* $\mathrm{div}(F) \geq D$. *If* $\mathcal{P} = \bigcup(\mathrm{Supp}\ (\mathrm{div}(f)) \setminus \mathrm{Supp}\ (\mathrm{div}(F))$ *for all* $f \in L(D)^*$ *then* $(V, \mathcal{P}, \mathcal{C})$ *is a symmetric set of curves, where* $\mathcal{C} = \{f \cdot F : f \in L(D)^*\}$.

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 $\mathrm{div}(f) = \alpha p + \beta q + R_1$ for any distinct two points $p, q \in \mathcal{P}$ such that $p, q \notin \mathrm{Supp}\ R_1$. Then we have

$$\mathrm{div}(f \cdot F) = \mathrm{div}(f) + \mathrm{div}(F) = \alpha p + \beta q + R_2\ ,\ p, q \notin \mathrm{Supp}\ R_2$$

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

$$|\{f \cdot F : I_p(f \cdot F, V) = \alpha, f \in L(D)^*\}| = |\{f \in L(D)^* : \mathrm{ord}_p(f) = \alpha\}|$$

and

$$\begin{aligned} & |\{f \cdot F : I_p(f \cdot F, V) = \alpha, I_q(f \cdot F, V) = \beta\, f \in L(D)^*\}| \\ = \ & |\{f \in L(D)^* : \mathrm{ord}_p(f) = \alpha, \mathrm{ord}_q(f) = \beta\}|. \end{aligned}$$

Let $D_p(\alpha) = D - \alpha p$ and $D_{q,r}(\alpha, \beta) = D - (\alpha q + \beta r)$, where $p, q, r \in \mathcal{P}$. We can easily see that

$$|\{f \in L(D)^* : \mathrm{ord}_p(f) = \alpha\}| = |L(D_p(\alpha))| - |L(D_p(\alpha + 1))| \tag{2.1}$$

and

$$\begin{aligned} & |\{f \in L(D)^* : \mathrm{ord}_p(f) = \alpha, \mathrm{ord}_q(f) = \beta\}| \\ = \ & |L(D_{p,q}(\alpha, \beta))| - |L(D_{p,q}(\alpha + 1, \beta))| - |L(D_{p,q}(\alpha, \beta + 1))| \\ & + |L(D_{p,q}(\alpha + 1, \beta + 1))|. \end{aligned} \tag{2.2}$$

When the genus $g = 0$, we can evaluate all dimensions of $L(D_{p,q}(\alpha, \beta))$ from the Riemann-Roch theorem for any pair (p, q) of distinct points and any pair (α, β) of integers. Since the cardinality (2.1) and (2.2) are not depend on points p, q chosen, $(V, \mathcal{P}, \mathcal{C})$ is a symmetric set of curves. □

Next we consider the case of the genus $g \geq 1$. For a divisor D such that $0 \leq \deg D \leq 2g - 2$, the dimension of $L(D)$ can not be obtained from the 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 manner as the proof of theorem 2.1, 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 $(V, \mathcal{P}, \mathcal{C})$ 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 $\mathcal{P}$.

THEOREM 2.2. *Let V be a non-singular curve with the genus $g \geq 1$, let D be an effective divisor on V and F a curve such that* $\mathrm{div}(F) \geq D$. *Suppose* $\mathcal{P} = \bigcup(\mathrm{Supp}\ (\mathrm{div}(f)) \setminus \mathrm{Supp}\ (\mathrm{div}(F))$ *for all $f \in L(D)^*$. If $M(p, q; \alpha, \beta)$ is independent of points for any pair (α, β) then $(V, \mathcal{P}, \mathcal{C})$ is a symmetric set of curves, where $\mathcal{C} = \{f \cdot F : f \in L(D)^*\}$.*

The necessary condition of the above theorem requires to prove for all pairs (α, β) whether $M(p, q; \alpha, \beta)$ is independent of points. We show that the number of checking is reducible in the next corollary.

COROLLARY 2.3. *If $M(p, q; \alpha, \beta)$ is independent of points for (α, β) satisfying* $\deg D - 2g + 2 \leq \alpha + \beta \leq \deg D$, *then $(V, \mathcal{P}, \mathcal{C})$ is a symmetric set of curves.*

PROOF. Let $D_{p,q}(\alpha, \beta) = D - (\alpha p + \beta q)$. If $\deg D - 2g + 2 \leq \alpha + \beta \leq \deg D$ then $0 \leq \deg D_{p,q}(\alpha, \beta) \leq 2g - 2$ and the dimension of $L(D_{p,q}(\alpha, \beta))$ can not be

obtained from Riemann-Roch theorem. Let $N(\alpha,\beta) = \{(\alpha',\beta') : \alpha' \geq \alpha, \beta' \geq \beta, \alpha'+\beta' < \deg D\}$. 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 $\deg D - 2g + 2 \leq \alpha'+\beta' \leq \deg D$, then $|L(D_{p,q}(\alpha,\beta))|$ is also independent of points p and q chosen. Hence, from (2.2) in the proof of theorem 2.1, we can conclude that $M(p,q;\alpha,\beta)$ is independent of points for any pair $(\alpha.\beta)$. □

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

$$\begin{cases} x = x_0 + t \\ y = y_0 + h(t), \end{cases} \tag{2.3}$$

where

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

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

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

In general case of the genus $g \geq 1$, it is not easy to find a point set $\mathcal{P}$ and a curve set $\mathcal{C}$ satisfying the necessary condition of the above theorem 2.2 or its corollary 2.3. We next consider a case that V is an elliptic curve, say $g = 1$.

3. Construction on an elliptic curve

Suppose, in this section, F_q is a finite field with odd characteristic and F_{q^m} is an extension of F_q. Let E be a non-singular elliptic curve defined over F_q given by the equation

$$F(x,y) = x^3 + ax^2 + bx + c - y^2.$$

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

THEOREM 3.1. *Let $\mathcal{C}$ be the set of all conics over F_{q^m}. Let $\mathcal{P}$ be the set of all F_{q^m}-rational intersection points of E and 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 an equation*

$$9x^4 + 12ax^3 + (4a^2+6b)x^2 + 4abx + b^2 - 4(a+3x)y^2 = 0, \tag{3.1}$$

where a, b and c are coefficients of F, then $(E,\mathcal{P},\mathcal{C})$ is a symmetric set of curves.

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

Let C be a conic defined by $G(x,y) = g_1x^2 + g_2y^2 + g_3xy + g_4x + g_5y + g_6 = 0$. By substituting (2.3) into G, we have

$$G(x_0 + t, y_0 + h(t)) = \mathbf{g}A\mathbf{t}, \tag{3.2}$$

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 a matrix B.) Let $C(p,q;\alpha,\beta) = \{C \in \mathcal{C} : I_p(C,E) \geq \alpha, I_q(C,E) \geq \beta\}$. $C(p,q;\alpha,\beta)$ is a linear space of curves. Let $A(p;\alpha)$ be the submatrix of the first α columns of A^t obtained by substituting p into (3.2). $\dim C(p,q;\alpha,\beta)$ 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 (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 $\det A(p;6)$ is

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

Moreover we have $\dim C(p,q;3,3) = 1$ because the determinant of the matrix $[A(p;3), A(q;3)]$ is 0. From the result 1.2, $C(p,q;\alpha,\beta) = \{0\}$ for any pair (α,β) satisfying $\alpha+\beta \geq 7$. From the result 1.3, $\dim C(p,q;\alpha,\beta) = 1$ 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

$$\dim C(p,q;5,1) = \dim C(p,q;4,2) = \dim C(p,q;2,4) = \dim C(p,q;1,5) = 0.$$

Hence, $M(p,q;\alpha,\beta)$ is independent of points for any pairs (α,β) satisfying $\alpha+\beta = 6$.

The elliptic curve E is given by

$$F(x,y) = x^3 + ax^2 + bx + c - y^2 = 0.$$

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

$$\begin{aligned} & (c + bx_0 + ax_0^2 + x_0^3 - y_0^2) + (b + 2ax_0 + 3x_0^2 - 2y_0y_1)t + (a + 3x_0 - y_1^2)t^2 \\ + \; & (1 - 2y_0y_3)t^3 + (-2y_1y_3 - 2y_0y_4)t^4 + (-2y_1y_4 - 2y_0y_5)t^5 \\ + \; & (-y_3^2 - 2y_1y_5 - 2y_0y_6)t^6 + \cdots \\ = \; & 0. \end{aligned}$$

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

$$\begin{cases} b + 2ax_0 + 3x_0^2 - 2y_0y_1 = 0 \\ a + 3x_0 - y_1^2 = 0 \end{cases}$$

which is equivalent to the equation (3.1). Therefore the point (x_0, y_0) is on the curve E' defined by the equation (3.1). □

We show here an example which constructs a symmetric set of curves obtained from the theorem 3.1. Let E be an 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 intersection points of E and a curve given by

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

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

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

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

Let $C(p,q;\alpha,\beta) = \{C \in \mathcal{C} : I_p(C,E) \geq \alpha, I_q(C,E) \geq \beta\}$. We can say that $\dim C(p,q;6,0) = \dim C(p,q;3,3) = \dim C(p,q;0,6) = 1$ and $\dim C(p,q;5,1) = \dim C(p,q;4,2) = \dim C(p,q;2,4) = \dim C(p,q;1,5) = 0$ for any pair (p,q) of points of $\mathcal{P}$. Hence $(V,\mathcal{P},\mathcal{C})$ 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 $|\mathcal{C}| = (5^2)^6$.

References

1. I. M. Chakravarti, *Fractional replication in asymmetrical factorial designs and partially balanced arrays*, Sankhyā 17 (1956), 143–164.
2. R. Fuji-Hara and S. Kuriki, *Mutually balanced nested designs*, Discrete Math. 97 (1991), 167–176.
3. William Fulton, *Algebraic curves : an introduction to algebraic geometry*, Mathematics lecture note series, Benjamin, 1969.
4. S. Kuriki and R. Fuji-Hara, *Balanced arrays of strength two and nested (r,λ)-designs*, J. Combin. Designs 2 (1994), 407–414.
5. Alfred Menezes, *Elliptic curve public key cryptosystems*, Kluwer Academic Publishers, 1993.
6. Carlos Moreno, *Algebraic curves over finite fields*, Cambridge University Press, New York, 1991.
7. Joseph H. Silverman and John Tate, *Rational points on elliptic curves*, Undergraduate texts in mathematics, Springer-Verlag, New York, 1992.
8. J. N. Srivastava, *Some general existence conditions for balanced arrays of strength t and 2 symbols*, J. Combinatorial Theory (A) 13 (1972), 198–206.

INSTITUTE OF POLICY AND PLANNING SCIENCES, UNIVERSITY OF TSUKUBA, TSUKUBA, IBARAKI, 305 JAPAN

E-mail address: fujihara@sk.tsukuba.ac.jp

DOCTORAL PROGRAM IN POLICY AND PLANNING SCIENCES, UNIVERSITY OF TSUKUBA, TSUKUBA, IBARAKI, 305 JAPAN

E-mail address: sshinoha@sk.tsukuba.ac.jp