HIROSHIMA MATH. J.
25 (1995), 43–52

Orthogonal matrices obtained from hypergeometric series over finite fields and elliptic curves over finite fields

Masao KOIKE

(Received August 17, 1993)

Abstract

We show that the semi-cyclic matrices attached to some hypergeometric series over finite fields are orthogonal. This proves Namba's conjecture. We also show that for certain family of elliptic curves, their trace of the Frobenius map are equal to special values of hypergeometric series over finite fields.

1. Introduction

Let $\mathbf{F}$ denote the finite field with q elements where $q = p^n$ and p is an odd prime. Then $\mathbf{F}^\times$ is a cyclic group of order $q - 1$ generated by a primitive element r. Put $m = (q - 1)/2$.

For a function $f: \mathbf{F}^\times \to \mathbf{C}$, we define

$$c_i = f(r^i) - f(-r^i) \qquad \textit{for } i = 0, 1, \cdots, m - 1 .$$

The semi-cyclic matrix Φ of size $m \times m$ attached to f is defined by

$$\Phi = \begin{pmatrix} c_0 & c_1 & c_2 & \cdots & c_{m-1} \\ -c_{m-1} & c_0 & c_1 & \cdots & c_{m-2} \\ -c_{m-2} & -c_{m-1} & c_0 & \cdots & c_{m-3} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ -c_1 & -c_2 & -c_3 & \cdots & c_0 \end{pmatrix}$$

In this paper, we shall show that the orthogonality of these matrices are described by means of the Mellin transform[1] of f, which is defined by the following; for any multiplicative character $\chi: \mathbf{F}^\times \to \mathbf{C}$, the Mellin transform $M_f(\chi)$ of f is defined by

$$M_f(\chi) = \sum_{t \in \mathbf{F}^\times} \chi(t) f(t) .$$

We shall prove

[1] This notion is defined in [2]

THEOREM 1.1. *The following conditions are equivalent.*
(A) ${}^t\Phi\cdot\Phi=\alpha 1_m,\ \alpha\in\mathbf{C}^\times$.
(B) $M_f(\chi)M_f(\bar{\chi})=\alpha$, *for all odd characters* χ *of* $\mathbf{F}^\times$.

Hypergeometric series over finite fields can provide us many examples satisfying the above condition (B). For example, we have

THEOREM 1.2. *Let* ψ *be an even character of* $\mathbf{F}^\times$, $\psi\neq\varepsilon$. *Then*

$$ {}_2F_1\left(\begin{matrix}\psi, & \bar{\psi} \\ & \varepsilon\end{matrix}\ \middle|\ x\right) $$

satisfies the condition (B).

2. Proof of Theorem 1.1

Throughout this paper, Greek letters χ, ψ, η, $\cdots$ will denote multiplicative characters of $\mathbf{F}^\times$. The trivial character and the quadratic character will be denoted by ε and ϕ respectively.

For any odd character χ of $\mathbf{F}^\times$, we put the vector v_χ:

$$ v_\chi={}^t(\chi(1),\chi(r),\cdots,\chi(r^{m-1})) $$

The following lemma may be well known and is easily proved:

LEMMA 2.1. *For any odd character* χ *of* $\mathbf{F}^\times$, v_χ *is an eigenvector of* Φ *with the eigenvalue* $M_f(\chi)$.

Let $S=(\chi_1,\cdots,\chi_m)$ denote the set of all odd characters of $\mathbf{F}^\times$. If m is even, then $\phi\notin S$ and if m is odd, $\phi\in S$. Hence we may assume the following:

If m is even, $\overline{\chi_i}=\chi_{m+1-i}$ for all i.

If m is odd, $\chi_1=\phi$ and $\overline{\chi_i}=\chi_{m+2-i}$ for all i, $2\leq i\leq m$.

Let W and Ψ be

$$ W=\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \chi_1(r) & \chi_2(r) & \cdots & \chi_m(r) \\ \vdots & \vdots & & \vdots \\ \chi_1(r^{m-1}) & \chi_2(r^{m-1}) & \cdots & \chi_m(r^{m-1}) \end{bmatrix} $$

$$ \Psi=\begin{bmatrix} M_f(\chi_1) & & & \\ & M_f(\chi_2) & & \\ & & \ddots & \\ & & & M_f(\chi_m) \end{bmatrix} $$

Then the above lemma shows that

$$\Phi\cdot W = W\cdot\Psi\,.$$

The orthogonal relations of characters imply that

$$
\begin{aligned}
{}^tW\cdot W &= \begin{bmatrix} & & m \\ & \cdot^{\cdot^{\cdot}} & \\ m & & \end{bmatrix} \qquad \text{if } m \text{ is even}\,,\\
&= \left[\begin{array}{c|ccc} m & & & \\ \hline & & & m \\ & & \cdot^{\cdot^{\cdot}} & \\ & m & & \end{array}\right] \qquad \text{if } m \text{ is odd}\,,
\end{aligned}
$$

and

$$
W^{-1} = \frac{1}{m}\begin{bmatrix} 1 & \bar{\chi}_1(r) & \cdots & \bar{\chi}_1(r^{m-1}) \\ 1 & \bar{\chi}_2(r) & \cdots & \bar{\chi}_2(r^{m-1}) \\ \vdots & \vdots & & \vdots \\ 1 & \bar{\chi}_m(r) & \cdots & \bar{\chi}_m(r^{m-1}) \end{bmatrix}.
$$

Therefore

$$
{}^tW\cdot{}^t\Phi\cdot\Phi\cdot W = {}^t\Psi\cdot{}^tW\cdot W\cdot\Psi
$$

$$
= \begin{cases}
\begin{bmatrix} & & mM_f(\chi_1)M_f(\chi_m) \\ & \cdot^{\cdot^{\cdot}} & \\ mM_f(\chi_m)M_f(\chi_1) & & \end{bmatrix} & \text{if } m \text{ is even}\,,\\[2ex]
\left[\begin{array}{c|ccc} mM_f^2(\phi) & & & \\ \hline & & & mM_f(\chi_2)M_f(\chi_m) \\ & & \cdot^{\cdot^{\cdot}} & \\ & mM_f(\chi_m)M_f(\chi_2) & & \end{array}\right] & \text{if } m \text{ is odd}\,.
\end{cases}
$$

Hence we get the proof of Theorem 1.1.

3. Hypergeometric series over finite fields

Here we shall prove Theorem 1.2.

The hypergeometric series over finite fields are first extensively studied by Greene [1] and we use the same notation as in his paper. Here we only use hypergeometric series of degree 2, which is defined by

$$
{}_2F_1\begin{pmatrix} A, & B \\ & C \end{pmatrix} \,\Big|\, x\Big) = \varepsilon(x)\frac{BC(-1)}{q}\sum_{y\in\mathbf{F}} B(y)\bar{B}C(1-y)\bar{A}(1-xy)\,.
$$

Its Fourier expansion is given by

$$ {}_2F_1\left(\begin{matrix} A, & B \\ & C \end{matrix} \mid x\right) = \frac{q}{q-1}\sum_{\chi}\binom{A\chi}{\chi}\binom{B\chi}{C\chi}\chi(x) . $$

Let f be a function over $\mathbf{F}^{\times}$ and its Fourier expansion is given by

$$ f(x) = \sum_{\chi} c(\chi)\chi(x) . $$

Then the Mellin transform of f is given by

$$ M_f(\chi) = (q-1)c(\bar{\chi}) . $$

Since the Fourier expansion of hypergeometric series is already known as above, its Mellin transform is also known explicitly. As a function $f(x)$ over $\mathbf{F}^{\times}$ considered in the previous sections, we take the hypergeometric series $f(x) = {}_2F_1\left(\begin{matrix} A, & B \\ & C \end{matrix} \mid x\right)$.

Then we have

$$ M_f(\chi) = qABC(-1)\binom{\chi}{A}\binom{\bar{C}\chi}{B\bar{C}} . $$

For the later application, we assume that

$$ A = \psi , \qquad B = \bar{\psi} , \qquad C = \varepsilon . $$

where ψ is not trivial. Then, in this case, we have

$$ M_f(\chi) = q\binom{\chi}{\psi}\binom{\chi}{\bar{\psi}} . $$

LEMMA 3.1. *For any χ such that $\chi \neq \psi$, $\bar{\psi}$, ε, we have*

$$ M_f(\chi)M_f(\bar{\chi}) = 1 . $$

PROOF. Using the formula (2.15) in Greene [1], we can see

$$ \binom{\chi}{\psi}\binom{\bar{\chi}}{\bar{\psi}} = \frac{1}{q} , $$

under the above condition on χ, and the result follows. $\square$

Similarly, we can prove following two lemmas.

LEMMA 3.2. *Assume that $\psi \neq \phi$. Then*

$$ M_f(\psi)M_f(\bar{\psi}) = \frac{1}{q} . $$

LEMMA 3.3. *Assume that* $\psi = \phi$. *Then*

$$M_f(\phi) = \frac{1}{q}.$$

Lemma 3.1 leads to the proof of Theorem 1.2 as follows; assume that ψ is an even character. Then the set S of all odd characters of $\mathbf{F}^\times$ does not contain ψ and $\overline{\psi}$, so all $\chi \in S$ satisfy the assumption in Lemma 3.1. Hence the condition (B) is proved to be true.

Lemma 3.2 and 3.3 are used to show that semi-cyclic matrices are not really orthogonal in some cases which are treated in later sections.

As interesting examples, we give four cases in which Φ has rational coefficients. We denote by $\tilde{\omega}$ a generator of the character group of $\mathbf{F}^\times$.
Case 1. $q \equiv 1 \pmod 4$ *and* $\psi = \phi = \tilde{\omega}^{(q-1)/2}$.
Case 2. $q \equiv 1 \pmod 3$ *and* $\psi = \tilde{\omega}^{(q-1)/3}$.
Case 3. $q \equiv 1 \pmod 8$ *and* $\psi = \tilde{\omega}^{(q-1)/4}$.
Case 4. $q \equiv 1 \pmod{12}$ *and* $\psi = \tilde{\omega}^{(q-1)/6}$.

It is clear that the congruence conditions for q imply that ψ are even in all the above cases, so we can apply Theorem 1.2.

PROPOSITION 3.1. *In the above cases,* $q \cdot {}_2F_1\begin{pmatrix} \psi, & \overline{\psi} & \\ & \varepsilon & \end{pmatrix}\!\!\mid x\Big)$ *are rational integers for all* $x \in \mathbf{F}^\times$.

PROOF. Let $\sigma \in \mathbf{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Then it is clear that

$${}_2F_1\left(\begin{matrix} \psi, & \overline{\psi} \\ & \varepsilon \end{matrix} \mid x\right)^\sigma = {}_2F_1\left(\begin{matrix} \psi^\sigma, & \overline{\psi}^\sigma \\ & \varepsilon \end{matrix} \mid x\right)$$

In the above cases, the set $\{\psi, \overline{\psi}\}$ coincides with $\{\psi^\sigma, \overline{\psi}^\sigma\}$ for all $\sigma \in \mathbf{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Using Theorem 3.20 in [1], we see that

$${}_2F_1\left(\begin{matrix} \psi^\sigma, & \overline{\psi}^\sigma \\ & \varepsilon \end{matrix} \mid x\right) = {}_2F_1\left(\begin{matrix} \psi, & \overline{\psi} \\ & \varepsilon \end{matrix} \mid x\right).$$

Hence, combining these two identities, these values are proved to be rational. From the definition, it is easily seen that the values in the proposition are algebraic integers, so the rationality implies that these values are rational integers. $\square$

REMARK 3.1. *Let* ψ *be a non trivial even character. Let* ψ_i, $1 \le i \le n$ *be all the conjugate characters of* ψ. *Then the same argument as above shows that*

$$ {}_nF_{n-1}\left(\begin{matrix}\psi_1, & \psi_2, & \cdots, & \psi_n \\ & \varepsilon, & \cdots, & \varepsilon\end{matrix} \mid x\right) $$

satisfies the condition (B).

4. Elliptic curves

The origin of semi-cyclic orthogonal matrices is in Namba [6]. His interest comes from the study of elliptic curves over the finite fields $\mathbf{F}_p$ with p elements. To compute the number of rational points of certain elliptic curves, he used the fact that the trace of the Frobenius map of this elliptic curve is congruent mod p to the special value of Legendre polynomials which is related to hypergeometric series. Thus he computed many examples and obtained serveral conjectures on semi-cyclic matrices, one of which is relevant to our Theorem 1.2.

We shall explain his conjecture and its relation to our theorem.

For any $\lambda \in \mathbf{F}_p$, $\lambda \neq 0$, 1, we consider the elliptic curves E_λ of the form:

$$ E_\lambda : y^2 = x(x-1)(x-\lambda) . $$

Then the number of $\mathbf{F}_p$-rational points of E_λ which is denoted by N_λ is given by

$$ \begin{aligned} N_\lambda &= 1 + \sum_{t \in \mathbf{F}_p} \{1 + \phi(t(t-1)(t-\lambda))\} \\ &= 1 + p + \sum_{t \in \mathbf{F}_p} \phi(t)\phi(t-1)\phi(t-\lambda) \end{aligned} $$

Therefore the trace $a_p(\lambda)$ of the Frobenius map is

$$ \begin{aligned} a_p(\lambda) &= 1 + p - N_\lambda \\ &= -\phi(-1)p \; {}_2F_1\left(\begin{matrix}\phi, & \phi \\ & \varepsilon\end{matrix} \mid \lambda\right). \end{aligned} $$

Defining $a_p(1)$ so that the above equality holds for $\lambda = 1$ too, Namba considered $a_p(\lambda)$ as a function on $\mathbf{F}_p^\times$ and computed the semi-cyclic matrix attached to this function. He conjectured that this matrix satisfies the condition (A) if $p \equiv 1 \pmod 4$.

Since the above equality shows that the semi-cyclic matrix in **Case 1** is constant times of Namba's one, so his conjecture is proved to be true by Theorem 1.2.

When $p \equiv 3 \pmod 4$, Namba found that the semi-cyclic matrix does not satisfy the condition (A). From our point of view, this is so because ϕ is odd.

PROPOSITION 4.1. *The notation being the same as in the previous section, we consider the following case that* $q \equiv 3 \pmod 4$ *and* $\psi = \phi$. *Then the semi-cyclic matrix* Φ *satisfies the following*:

$$ {}^t\Phi \cdot \Phi = 1_m - \frac{2(q+1)}{q^2}\Omega , $$

where Ω *is the matrix of size* $m \times m$ *whose* (i,j) *component is* $\phi(r^{i+j})$.

PROOF. The argument is similar to the proof of Theorem 1.2. Only the difference is that ϕ belongs to S and $M_f(\phi)M_f(\phi) = \frac{1}{q^2}$ by Lemma 3.3. □

In [6], he also considered another family of elliptic curves E_λ^1:

$$ E_\lambda^1 : y^2 = x^3 + x^2 - \frac{4\lambda}{27}, $$

$\lambda \in \mathbf{F}_p$, $\lambda \neq 0, 1$.

Like the above case, he considered the trace $a_p(1, \lambda)$ of the Frobenius map of E_λ^1 as a function on $\mathbf{F}_p^\times$ and computed semi-cyclic matrices attached to this function and got similar conjectures. To prove his conjectures, we shall show that $a_p(1, \lambda)$ is written by hypergeometric series in **Case 4** in the next sections.

5. Estimate of values of hypergeometric series

For any $\lambda \in \mathbf{F}$, $\lambda \neq 0, 1$, we consider the elliptic curve E_λ over $\mathbf{F}$

$$ E_\lambda : y^2 = x(x-1)(x-\lambda) $$

Let $a_q(\lambda)$ denote the trace of qth-Frobenius map of E_λ. Then, by the same argument as in the previous section, we get

$$ a_q(\lambda) = -q\phi(-1) \cdot {}_2F_1\begin{pmatrix} \phi, & \phi \\ & \varepsilon \end{pmatrix} \mid \lambda \Big). $$

The well-known estimate of the number of $\mathbf{F}$-rational points of E_λ implies

$$ |a_q(\lambda)| \leq 2\sqrt{q} . $$

Hence we get

$$ \left| q \cdot {}_2F_1\left(\begin{matrix} \phi, & \phi \\ & \varepsilon \end{matrix} \mid \lambda \right) \right| \leq 2\sqrt{q} . $$

This estimate holds for $\lambda = 1$ too.

Proposition 5.1. *Let ψ be any character in the four cases in the section 3. Then we have the following estimate*:

$$\left| q \cdot {}_2F_1\begin{pmatrix} \psi, & \overline{\psi} & \\ & \varepsilon & \end{pmatrix} \Big| \, x \right| \leq \begin{cases} 2\sqrt{q} & \textit{in } \textbf{Cases 1, 2}, \\ 4\sqrt{q} & \textit{in } \textbf{Case 3}, \\ 8\sqrt{q} & \textit{in } \textbf{Case 4} \end{cases}$$

for all x in $\mathbf{F}^\times$.

Remark 5.1. *The above estimate is temporary. If hypergeometric series are defined over the finite field $\mathbf{F}_p$, the precise one will be given in Corollary 6.1.*

Proof. Concerning to **Case 1**, we already prove this estimate by using Hasse's inequality for elliptic curves over finite fields.

For **Case 2**, we consider the following curve

$$y^3 = x(x-1)(x-\lambda)^2 .$$

Then the number N of $\mathbf{F}$-rational points of this affine curve is given by

$$N = q + 2q \cdot {}_2F_1\begin{pmatrix} \psi, & \overline{\psi} & \\ & \varepsilon & \end{pmatrix} \Big| \, \lambda \Big),$$

by using Proposition 3.1. Applying Theorem 6.57. in [4], we obtain the following estimate

$$|N - q| \leq 4\sqrt{q} .$$

Hence we get the proof for this case.

For **Case 3**, we consider the curve

$$y^4 = x(x-1)(x-\lambda)^3 .$$

Then the number N of $\mathbf{F}$-rational points of this affine curve is given by

$$N = q + 2q\psi(-1) \cdot {}_2F_1\begin{pmatrix} \psi, & \overline{\psi} & \\ & \varepsilon & \end{pmatrix} \Big| \, \lambda \Big) + q\phi(-1) \cdot {}_2F_1\begin{pmatrix} \phi, & \phi & \\ & \varepsilon & \end{pmatrix} \Big| \, \lambda \Big),$$

by using Proposition 3.1. too.

The estimate of the last term of the above equality is already known. Then applying Theorem 6.57 in [4], we obtain the proof for this case.

The proof for **Case 4** being similar to the above, we omit it. □

Remark 5.2. *The congruence conditions in these cases which assure that ψ are even are not needed for the above result.*

6. Elliptic curves again

In this section, all objects are defined over the finite field $\mathbf{F}_p$. Let $p \equiv 1 \pmod 3$ and put $f = \frac{p-1}{6}$ and assume that $p \geq 101$. For any $\lambda \in \mathbf{F}_p$ such that $\lambda \neq 0, 1$, we consider the elliptic curve E^1_λ:

$$E^1_\lambda : y^2 = x^3 + x^2 - \frac{4\lambda}{27}.$$

Let $a_p(1, \lambda)$ denote the trace of the Frobenius map of this elliptic curve. We define the polynomial $H_p(X) \in \mathbf{Z}[X]$ as follows:

$$H_p(x) = \sum_{n=0}^{f} \binom{f}{n} \binom{5f}{n} x^n$$

and put

$$\tilde{H}_p(X) = H_p(X) \pmod p.$$

In [5], it is shown that

$$a_p(1, \lambda) (\text{mod p}) = \tilde{H}_p(\lambda).$$

As in [3], we may consider the values of hypergeometric series p-adically. We denote by ω the Teichmüller character of $\mathbf{F}_p$. Put $\psi = \omega^{(p-1)/6}$.

By using the same argument as in the proof of Proposition 1 in [3], we can prove

$$-p \cdot {}_2F_1\left(\begin{matrix} \psi, & \bar{\psi} \\ & \varepsilon \end{matrix} \mid \lambda\right) \quad (\text{mod p}) = \tilde{H}_p(\lambda)$$

Hence we get

$$a_p(1, \lambda) \equiv -p \cdot {}_2F_1\left(\begin{matrix} \psi, & \bar{\psi} \\ & \varepsilon \end{matrix} \mid \lambda\right) \quad (\text{mod p})$$

The estimate of these two rational integers are known by Proposition 5.1 and by the Hasse's inequality, so they are equal since $p \geq 101$.

THEOREM 6.1. *The notation being as above, we assume that $p \geq 101$. Then we have*

$$a_p(1, \lambda) = -p \cdot {}_2F_1\left(\begin{matrix} \psi, & \bar{\psi} \\ & \varepsilon \end{matrix} \mid \lambda\right).$$

We can prove the following theorem by using the similar argument as above.

THEOREM 6.2. *Let* $p \equiv 1 \pmod 4$ *and put* $\eta = \omega^{(p-1)/4}$. *For any* $\lambda \in \mathbf{F}_p$ *such that* $\lambda \neq 0, 1$, *consider the elliptic curve*:

$$E_\lambda^2 : y^2 = x^3 + x^2 + \frac{\lambda}{4}x .$$

Then its trace of the Frobenius map is equal to

$$-p \cdot {}_2F_1\left(\begin{matrix}\eta, & \bar{\eta} \\ & \varepsilon\end{matrix} \mid \lambda\right).$$

As a corollary of these theorems, we get a more precise estimate of hypergeometric series than in Proposition 5.1.

COROLLARY 6.1. *The notation and assumptions are the same as above. Let* ψ *be any character in the four cases given in the section* 3. *Assume that* p *is greater than* 100. *Then we have the following estimate*:

$$\left| p \cdot {}_2F_1\left(\begin{matrix}\psi, & \bar{\psi} \\ & \varepsilon\end{matrix} \mid x\right)\right| \leq 2\sqrt{p} \qquad \text{for all } x \text{ in } \mathbf{F}_p^\times .$$

References

[1] John Greene, Hypergeometric functions over finite fields, Trans. A.M.S., **301** (1987), 77–101.

[2] John Greene, Hypergeometric functions over finite fields and representations of **SL**(2, *q*), preprint.

[3] M. Koike, Hypergeometric series over finite fields and Apéry numbers, Hiroshima Math. J., **22** (1992), 461–467.

[4] R. Lidl and Niederreiter, Finite fields, Encyclopedia of Math. and its appl., 20, Addison-Wesley Publishing Co., 1983.

[5] K. Namba, Legendre polynomial over finite fields and factorization of integers, Proc. Int. Symp., Hua Lookeng, Springer, 1991.

[6] K. Namba, Elliptic curves over finite fields and cyclotomic polynomials, preprint.

Department of Mathematics
Faculty of Science
Hiroshima University