East Asian Math. J.
Vol. 38 (2022), No. 5, pp. 611–616
http://dx.doi.org/10.7858/eamj.2022.037

JACOBIAN VARIETIES OF HYPERELLIPTIC CURVES WITH MIXED SYMMETRIC FORMAL TYPE

Gyoyong Sohn

Abstract. This paper considers the Jacobian variety of a hyperelliptic curve over a finite field with mixed symmetric formal type. We present the Newton polygon of the characteristic polynomial of the Frobenius endomorphism of the Jacobian variety. It gives a useful tool for finding the local decomposition of the Jacobian variety into isotypic components.

1. Introduction

The Newton polygon, p-rank and Ekedahl-Oort type are discrete invariants of an abelian variety in positive characteristic p. These give important information about abelian variety defined over finite fields (e.g., [2, 3] and [4]). In [5], Yui gaves the characterization of Jacobian variety of hyperelliptic curves with the help of the Cartier-Manin matrix of curve. In this paper, we consider the Jacobian variety of the hyperelliptic curve over finite field whose Cartier-Manin matrix has determinant zero. We show the Jacobian variety of hyperelliptic curve with new formal structure of the mixed symmetric type. The formal group of the Jacobian variety is the connected component of the p-divisible group of the Jacobian variety.

Let $\mathbb{F}_q$ be a finite field with $q = p^n$ elements for prime p. Let C be a hyperelliptic curve of genus g defined over $\mathbb{F}_q$ and J_C denote its Jacobian variety. Let $M_r = \sharp C(\mathbb{F}_{q^r})$ be the number of points of C defined over $\mathbb{F}_{q^r}$, for $r \geq 1$. The *zeta function of* C is

$$Z(C/\mathbb{F}_q, t) = \exp\Big(\sum_{r=1}^{\infty} M_r t^r/r\Big).$$

By the Weil conjectures for curves [6, 7], the zeta function $Z(C/\mathbb{F}_q, t)$ can be written as

$$Z(C/\mathbb{F}_q, t) = \frac{L(C/\mathbb{F}_q, t)}{(1-t)(1-qt)},$$

Received April 29, 2022; Accepted September 15, 2022.
2010 *Mathematics Subject Classification.* 11C10, 11G10, 11G25.
Key words and phrases. Hyperellitpic curves over finite fields.

(pISSN 1226-6973, eISSN 2287-2833)

where $L(C/\mathbb{F}_q, t)$ is the L-polynomial of C. Let $T_l(J_C)$ be the l-th Tate module of J_C and $V_l(J_C) = T_l(J_C) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ be the corresponding vector space over $\mathbb{Q}_l$. For $l \neq p$, the characteristic polynomial of the Frobenious endomorphism π_{J_C} of J_C is defined as

$$P(J_C/\mathbb{F}_q, t) = \det(\pi_{J_C} - tI_d \mid V_l(J_C)).$$

Then $P(J_C/\mathbb{F}_q, t) = t^{2g} L(C/\mathbb{F}_q, t)$. Furthermore, $L(C/\mathbb{F}_q, t)$ is factored as

$$L(C/\mathbb{F}_q, t) = \prod_{i=1}^{g} (1 - \alpha_i t)(1 - \overline{\alpha}_i t),$$

where each α_i is a complex number of absolute value $\sqrt{q}$ and $\overline{\alpha}_i$ denotes the complex conjugate of α_i. Moreover, $P(J_C/\mathbb{F}_q, t)$ is a monic polynomial of degree $2g$ with rational integer coefficients of the form

(1)
$$P(J_C/\mathbb{F}_q, t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_g t^g + q a_{g-1} t^{g-1} + \cdots + q^{g-1} a_1 t + q^g,$$

for all $a_i \in \mathbb{Z}$, $1 \leq i \leq g$. For simplicity, we write $P(t)$ instead of $P(J_C/\mathbb{F}_q, t)$.

Remark 1. Let v_p be the p-adic valuation of $\mathbb{Q}_p$ and let ν_p denote the unique extension of the p-adic valuation v_p to the algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, normalized so that $\nu_p(p) = 1$. The Newton polygon of $P(t) = \sum_{i=0}^{2g} a_i t^i \in \mathbb{Z}[t]$ over $\mathbb{Q}_p$ is the lower envelope of the set of the points $\{(i, v_p(a_i)) | 0 \leq i \leq 2g\}$ in $\mathbb{R} \times \mathbb{R}$.

2. Cartier-Manin matrix

In this section, we recall the definition of the Cartier-Manin matrix in the case of hyperelliptic curves. Let $K = \mathbb{F}_q(C)$ be a function field of C of one variable over $\mathbb{F}_q$ and let K^p denote the subfield of p-th powers. Let Ω_K be the space of all differential forms of degree 1 on K and let x be a separably generating transcendental element in $K \backslash K^p$. Then every differential $\omega \in \Omega_K$ can be written uniquely as

$$\omega = d\lambda + a^p x^{p-1} dx,$$

with $\lambda, a \in K$, $a^p \in K^p$. The *(modified) Cartier operator* $\mathcal{C} : \Omega_K \to \Omega_K$ is defined as $\mathcal{C}(x) = a dx$.

Let $\omega = (\omega_1, \ldots, \omega_g)$ be a basis of Ω_K. Then there is $g \times g$ matrix $A = (a_{i,j})$ with coefficients in $\mathbb{F}_q$ such that

$$\mathcal{C}(\omega) = A^{(1/p)} \omega,$$

where $A^{1/p}$ denotes $a_{i,j}^{1/p}$. The matrix A is called the *Cartier-Manin matrix* of the hyperelliptic curve C.

In [1], Manin showed that this matrix is related to the characteristic polynomial of the Frobenius endomorphism π_{J_C} modulo p. Then, we have the following theorem.

Theorem 2.1. *Let C be a curve of genus g defined over a finite field $\mathbb{F}_{p^n}$. Let A be the Cartier-Manin matrix of C and let $A_\pi = AA^{(p)}A^{(p^2)}\cdots A^{(p^{n-1})}$. Let $\kappa(t)$ be the characteristic polynomial of the matrix A_π and $\chi(t)$ the characteristic polynomial of the Frobenius endomorphism of J_C. Then, we have*

$$\chi(t) \equiv (-1)^g t^g \kappa(t) \ (mod\ p).$$

Proof. See [1]. □

Note that this theorem provides a very efficient method to compute the characteristic polynomial of the Frobenius endomorphism and the group order of the Jacobian of C modulo p.

3. Jacobian variety of C

In this section, we present the Newton polygon of the characteristic polynomial of the Frobenius endomorphism of J_C with mixed symmetric formal type.

In [5], Yui gave a complete characterization of the ordinary Jacobian variety J_C of C whose Cartier-Manin matrix has determinant zero in $\mathbb{F}_q$. In the case of determinant $|A| = 0$, there are useful results to determine the algebraic structure of Jacobian variety J_C of C. Now we discuss the Jacobian variety J_C of C whose A has determinant zero in $\mathbb{F}_q$.

Theorem 3.1. *Suppose that the Cartier-Manin matrix A of C has the determinant $|A| = 0$ in $\mathbb{F}_q$ and the matrix $A_\pi = AA^{(p)}\cdots A^{(p^{n-1})}$ has rank 0. Then the characteristic polynomial $P(t)$ has the p-adic decomposition $P(t) = \prod_{i=1}^{2g}(t-\alpha_i)$ with $0 < \nu_p(\alpha_i) < n$.*

Theorem 3.1 gives a decomposition of $P(t)$ over $\mathbb{Q}_p$. Then we can factor $P(t)$ into the form

(2)

$$P(t) = \prod_{\substack{i=1 \\ \nu_p(\alpha_i)=n/2}}^{2s} (t-\alpha_i) \prod_{\substack{i=1, \\ \nu_p(\alpha_i)=0}}^{r} (t-\alpha_i)(t-\overline{\alpha}_i) \prod_{\substack{i=1, \\ 0<\nu_p(\alpha_i)<n/2}}^{g-s-r} (t-\alpha_i)(t-\overline{\alpha}_i),$$

where $2s$ (resp., r) the number of the p-adic roots α_i of $P(t)$ with $v_p(\alpha_i) = n/2$ (resp., 0). There are the algebraic structure of Jacobian variety J_C up to isogeny, in the cases $[s = g, r = 0]$, $[s = 0, r = 0]$, and $[0 < s < g, 0 < r < g]$, respectively. Now, we consider the Jacobian variety with the characteristic polynomial of mixed symmetric formal type in the case $[s = 0, r = 0]$.

Theorem 3.2. [5] *Suppose that the Cartier-Manin matrix A of C has the determinant $|A| = 0$ in $\mathbb{F}_q$ and the matrix $A_\pi = AA^{(p)}\cdots A^{(p^{n-1})}$ has rank 0. The following statements are equivalent :*
(a) $P(t) = \prod_{i=1}^{g}(t-\alpha_i)(t-\overline{\alpha}_i)$ with α_i simple roots and $\nu_p(\alpha_i) = n\lambda$, $0 < \lambda < \frac{1}{2}$ for every $1 \le i \le g$,

(b) $P(t) = \sum_{i=0}^{2g} a_i t^i$ *is a distinguished polynomial over* $\mathbb{Z}_p$ *and the coefficients* a_i *satisfy the condition:*

$$\min_{0\le i\le 2g} \frac{v_p(a_i)}{in} = \frac{v_p(a_g)}{gn} = \lambda = \frac{\mu_\lambda}{\mu_\lambda + \omega_\lambda},$$

where μ_λ, ω_λ *are positive integers such that* $1 \le \mu_\lambda < \omega_\lambda$, $(\mu_\lambda, \omega_\lambda) = 1$, *and* $\mu_\lambda + \omega_\lambda = g$.

Proof. See [5]. □

Now we consider the characteristic polynomial $P(t)$ of J_C with degree m for positive integer m.

Lemma 3.3. *The hypothesis and the notation are as in Theorem 3.2. Let* $P_A(t) = \prod_{i=1}^{m}(t-\alpha_i)(t-\overline{\alpha}_i)$ *with* α_i *complex numbers, and* $\nu_p(\alpha_i) = n\lambda$, $0 < \lambda < \frac{1}{2}$ *for* $1 \le i \le m$. *If* $P(t) = \sum_{i=0}^{2m} a_i t^i$ *is an equivalent polynomial over* $\mathbb{Z}_p$ *with related to* $P_A(t)$, *then the coefficients* a_i *satisfy the condition:*

$$v_p(a_m) = m\lambda n \text{ and } v_p(a_{(m-i)}) \ge (m-i)\lambda n$$

where

$$\lambda = \frac{\mu_\lambda}{\mu_\lambda + \omega_\lambda} \tag{3}$$

is a rational number such that $1 \le \mu_\lambda < \omega_\lambda$, $(\mu_\lambda, \omega_\lambda) = 1$, *and* $\mu_\lambda + \omega_\lambda = m$ *for positive integers* μ_λ, ω_λ.

Proof. Suppose that the characteristic polynomial $P(t)$ has the following form : $P(t) = \prod_{i=1}^{m}(t-\alpha_i)(t-\overline{\alpha}_i)$ with $\nu_p(\alpha_i) = \lambda n$, $0 < \lambda < \frac{1}{2}$ for $\lambda \in \mathbb{Z}$, $1 \le i \le m$. It is the case of $s = 0$ and $r = 0$ in (2). Put $\overline{\alpha}_i = \alpha_{m+i}$ for $1 \le i \le m$. Then we have $\nu_p(\alpha_i) = \lambda n$, $\nu_p(\alpha_{m+i}) = (1-\lambda)n$ for $1 \le i \le m$, from which we have that $v_p(a_0) = 0$, $v_p(a_i) \ge \lambda i n$ for every $1 \le i \le m$, $v_p(a_m) = m\lambda n$, and $v_p(a_{m+i}) \ge m\lambda n + (1-\lambda)in$ for $1 \le i \le m$. Hence it follows that

$$\frac{v_p(a_i)}{in} \ge \lambda, \ \frac{v_p(a_m)}{mn} = \lambda, \text{ and } \frac{v_p(a_{m+i})}{(m+i)n} \ge \lambda.$$

Therefore, we get

$$\min_{0\le i\le 2m} \frac{v_p(a_i)}{in} = \frac{v_p(a_m)}{mn} = \lambda.$$

Now put $\mu_\lambda = \lambda m$ and $\omega_\lambda = m - \mu_\lambda = (1-\lambda)m$. Then μ_λ, ω_λ are positive integers satisfying $1 \le \mu_\lambda < \omega_\lambda$, $\mu_\lambda + \omega_\lambda = m$, $(\mu_\lambda, \omega_\lambda) = 1$, and $\lambda = \mu_\lambda/(\mu_\lambda + \omega_\lambda)$. □

Our main result is the following theorem.

Theorem 3.4. *Suppose that the Cartier-Manin matrix* A *of* C *has the determinant* $|A| = 0$ *and the matrix* $A_\pi = AA^{(p)}\cdots A^{(p^{n-1})}$ *has rank 0. The following statements are equivalent :*

(a) The characteristic polynomial $P(t)$ *of Jacobian variety* J_C *is decomposed*

into the product $P_1(t)$ *and* $P_2(t)$, *where* $P_1(t) = \prod_{i=1}^{g-l}(t-\alpha_i)(t-\overline{\alpha}_i)$ *with* $\nu_p(\alpha_i) = \lambda_1 n$, $0 < \lambda_1 < 1/2$ *and* $P_2(t) = \prod_{i=1}^{l}(t-\alpha_i)(t-\overline{\alpha}_i)$ *with* $\nu_p(\alpha_i) = \lambda_2 n$ *for* $0 < \lambda_2 < 1/2$.

(b) The arbitrary polynomial over $\mathbb{Z}_p$ *is denoted by* $P(t) = \sum_{i=0}^{2g} a_i t^i$ *and the coefficients* a_i *satisfy the conditions:*

$$v_p(a_{g-l}) = (g-l)\lambda_1 n \text{ and } v_p(a_{g-l-j}) \geq (g-l-j)\lambda_1 n$$

for $1 \leq j \leq g-l-1$, *where* $\lambda_1 = \frac{\mu_{\lambda_1}}{\mu_{\lambda_1}+\omega_{\lambda_1}}$ *is a rational number satisfying* $1 \leq \mu_{\lambda_1} < \omega_{\lambda_1}$, $(\mu_{\lambda_1}, \omega_{\lambda_1}) = 1$, $\mu_{\lambda_1} + \omega_{\lambda_1} = l$ *for positive integers* μ_{λ_1}, ω_{λ_1}, *and*

$$v_p(a_{g-i}) \geq (g-l)\lambda_1 n + (l-i)\lambda_2 n$$

for $1 \leq i \leq l-1$, *where* $\lambda_2 = \frac{\mu_{\lambda_2}}{\mu_{\lambda_2}+\omega_{\lambda_2}}$ *is a rational number satisfying* $1 \leq \mu_{\lambda_2} < \omega_{\lambda_2}$, $(\mu_{\lambda_2}, \omega_{\lambda_2}) = 1$, $\mu_{\lambda_2} + \omega_{\lambda_2} = g - l$ *for* μ_{λ_2}, $\omega_{\lambda_2} \in \mathbb{Z}^+$, *and* $\lambda_1 > \lambda_2$.

Proof. Assume the condition (1). Then $P(t) = P_1(t)P_2(t)$ has the form

$$P(t) = \prod_{\substack{i=1,\\ \nu_p(\alpha_i)=\lambda_1 n}}^{g-l} (t-\alpha_i)(t-\overline{\alpha}_i) \prod_{\substack{i=1,\\ \nu_p(\alpha_i)=\lambda_2 n}}^{l} (t-\alpha_i)(t-\overline{\alpha}_i), \tag{4}$$

for $0 < \lambda_1, \lambda_2 < 1/2$. Let $P_1(t) = \sum_{i=1}^{2(g-l)} b_i t^i$ be an equivalent polynomial over $\mathbb{Z}_p$ related to $P_1(t)$ in (a). By Lemma 3.3, we consider the polynomials $P(t)$ in $\mathbb{Z}_p$ with degree $2(g-l)$ and $2l$, respectively. Then p-adic values b_i of $P_1(t)$ are $v_p(b_{g-l}) = (g-l)\lambda_1 n$, $v_p(b_{g-l-i}) \geq (g-l-i)\lambda_1 n$ where λ_1 satisfies condition (3) in Lemma 3.3. Let $P_2(t) = \sum_{i=1}^{2l} d_i t^i$ be an equivalent polynomial over $\mathbb{Z}_p$ related to $P_2(t)$ in (a). Then we have $v_p(b_l) = l\lambda_2 n$ and $v_p(d_{(l-i)}) \geq (l-i)\lambda_2 n$ where λ_2 satisfies condition (3).

The p-adic values of b_{g-l} and d_l are $v_p(b_{g-l}) = \sum_{i=1,\nu_p(\alpha_i)=\lambda_1 n}^{g-l} = \nu_p(\alpha_i) = (g-l)\lambda_1 n$ and $v_p(d_l) = \sum_{i=1,\nu_p(\alpha_i)=\lambda_2 n}^{l} = \nu_p(\alpha_i) = l\lambda_2 n$, respectively. Since $v_p(b_{g-l-j}) = v_p(a_{g-l-j})$, we have $v_p(a_{g-l-j}) \geq (g-l-j)\lambda_1 n$ for $1 \leq j \leq g-l-1$. The factorization $P(t) = P_1(t)P_2(t)$ gives

$$v_p(a_g) = v_p(b_{g-l}) + v_p(d_l) = (g-l)\lambda_1 n + l\lambda_2 n$$

and

$$v_p(a_{g-i}) \geq v_p(d_{l-i}) + v_p(b_{g-l}) = (l-i)\lambda_2 n + (g-l)\lambda_1 n,$$

for $1 \leq i \leq l-1$. □

Theorem 3.5. *If the characteristic polynomial* $P(t)$ *of the Jacobian variety* J_C *of* C *has the form* (4), *then the Newton polygon of* $P(t)$ *has the segments* L_1, L_2, L_3, L_4 *from the right with slopes* $-\lambda_1 n$, $-\lambda_2 n$, $-(1-\lambda_2)n$ *and* $-(1-\lambda_1)n$, *respectively. The Newton polygon of* $P(t)$ *is represented in Figure 1.*

Proof. By Theorem 3.4, the Newton polygon has the segments L_i, $1 \leq i \leq 4$ with line equations $y = -\lambda_1 nx + 2g\lambda_1 n$, $y = -\lambda_2 nx + (g+l)\lambda_2 n + (g-l)\lambda_1 n$, $y = -(1-\lambda_2)nx + gn + (g-l)n(\lambda_1 - \lambda_2)$ and $y = -(1-\lambda_1)nx + gn$ respectively. □

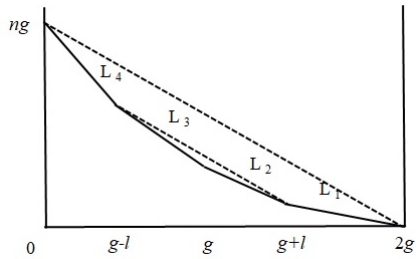

FIGURE 1.

References

[1] Yu. I. Manin, *The Hasse-Witt matrix of an algebraic curve*, AMS Trans. Ser. 2. (1965), no. 45, 245–264.
[2] F. Oort, *Hyperelliptic supersingular curves*, Arithmetic algebraic geometry (Texel, 1989), Progr. math., vol. 89, birkhäuser Boston, Boston, MA, 1991, pp. 247–284.
[3] R. Pries, *The p-torsion of curves with large p-rank*, Int. J. Number Theory. **5** (2009), no. 6, 1103–1116.
[4] J. Scholten and H. J. Zhu, *Hyperelliptic curves in characteristic 2*, Int. Math. Res. Not. (2002), no. 17, 905-917.
[5] N. Yui, *On the Jacobian varieties of hyperelliptic curves over fields of characteristic* $p > 2$, J. Algebra. **52** (1978), no. 2, 378–410.
[6] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041, Hermann et Cie.. Paris, 1948.
[7] A. Weil, *Variétés abéliennes et courbes algébriques*, Actualités Sci. Ind., no. 1064, Hermann & Cie., Paris, 1948.

GYOYONG SOHN
DEPARTMENT OF MATHEMATICS EDUCATION, DAEGU NATIONAL UNIVERSITY OF EDUCATION, DAEMYUNG 2-DONG, DAEGU, REPUBLIC OF KOREA
Email address: gysohn@dnue.ac.kr