ISOMORPHISM CLASSES OF HYPERELLIPTIC CURVES OF GENUS 2 OVER $\mathbb{F}_{2^n}$

Y.CHOIE AND E.JEONG
DEPARTMENT OF MATHEMATICS
POHANG UNIVERSITY OF SCIENCE AND TECHNOLOGY
POHANG, 790–784, KOREA
EMAIL: YJC, EKJEONG @POSTECH.AC.KR

Abstract. We give the exact number and representatives of the isomorphism, which preserves infinity, classes of hyperelliptic curves of genus 2 over finite fields with characteristic 2 in most cases. These results have applications to hyperelliptic curve cryptography.

Keywords hyperelliptic curves of genus 2, finite fields, isomorphism classes

1. Introduction

Since Koblitz suggested using the hyperelliptic curve H as a good source of public key cryptosystem, many interesting results have been explored toward hyperelliptic cryptosystem. Due to a subexponential algorithm by Adleman, DeMorrais and Huang[2] and that by Gaudry[8], hyperelliptic curve of genus $1, 2, 3$ can be very attractive for the cryptographic purpose. It may be useful, for cryptographic purpose, to classify the isomorphism classes of hyperelliptic curves of genus $1, 2$ and 3 over finite fields. The isomorphsim classes of elliptic curve over even characteristic fields were determined(see [14]).

In this paper we count the exact number of isomorphism classes of pointed hyperelliptic curves of genus 2, so hyperelliptic Weierstrass equations, over a field $\mathbb{F}_q$ with $q = 2^n$ and list all the representatives of isomorphism classes. In [9] the number of isomorphism classes of pointed hypereilliptic curves of genus 2 over $\mathbb{F}_q$ with characteristic different from 2 or 5 were studied. Later the bound of number of isomorphism classes over $\mathbb{F}_{2^n}$ was derived in [5]. On the other hand, in [4] the formulae for the number of curves of genus 2 over even characteristic fields with a fixed structure of ramification divisor has been derived.

This paper is organized as follows. In Section 2 we recall necessary definitions and give the notion of isomorphism between hyperelliptic curves. In Section 3 we give the exact number of all the isomorphism classes, with one exception on Type III case. Moreover, the tables which contain all the representatives of isomorphism classes are produced.

2. **Hyperelliptic curves**

In this section, we recall the basic definitions and theories basically given in [13].

A hyperelliptic curve over a field $\mathbb{F}$ of genus g is a nonsingular projective curve C over $\mathbb{F}$ of genus g for which there exists a map $C \longrightarrow \mathbb{P}^1(\mathbb{F})$ of degree two. When $g = 1$, C is an elliptic curve and the isomorphsim classes of elliptic curve over finite fields were determined(see [14]).

In this paper, we consider pointed hyperelliptic curves, which is defined in the following way; Let C be a hyperelliptic curve over $\mathbb{F}$ with $\mathbb{F}$-rational Weierstrass point P. Then the pair (C, P) is called hyperelliptic over $\mathbb{F}$. Thus, when $g = 1, (C, P)$ being hyperelliptic means that C is an elliptic curve with origin P. We denote the set of all hyperelliptic curves (C, P) over $\mathbb{F}$ of genus g by H_g.

Next, we consider the notion of Weierstrass equation;

Definition 2.1. *A Weierstrass equation E over $\mathbb{F}$ of genus g is*

$$E/\mathbb{F} : y^2 + h(x)y = f(x),$$

where $h, f \in \mathbb{F}[x]$, $deg(h) \le g$, $deg(f) = 2g + 1$, f is monic, and there are no singular points; a singular point on $E(x, y) = y^2 + h(x)y - f(x)$ is a solution $(x, y) \in \bar{\mathbb{F}} \times \bar{\mathbb{F}}$ which satisfies $E(x, y), E_x(x, y)$ and $E_y(x, y)$. We denote the set of all Weierstrass equations of genus g over $\mathbb{F}$ by W_g.

The following proposition corresponds a Weierstrss equation to hyperelliptic pair (C, P).

Proposition 2.2. [13] *Let (C, P) be hyperelliptic over $\mathbb{F}$ with genus g. Then there exist nonconstant functions $x, y \in \mathbb{F}(C)$ with $x \in L(2P), y \in L((2g + 1)P)$, which satisfy a Weierstrass equation of genus g over $\mathbb{F}$. Here, $L(D)$*

denotes the vector space of global sections of the line bundle associated to a divisor D. Moreover, such an equation is unique up to a change of coordinates of the form

$$(x,y)\longrightarrow(\alpha^2x+\beta,\alpha^{2g+1}y+t) \tag{2.1}$$

where $\alpha,\beta\in\mathbb{F}$ with $\alpha\neq 0$ and $t\in\mathbb{F}[x]$ with $deg(t)\leq g$.

Furthermore, a Weierstrass equation E arises from some (C,P) if and only if E has no singular points, and in this case the set of such E form an equivalence class of Weierstrass equations related by the e transformations (2.1).

So, we can say that there is a 1-1 correspondence between isomorphism classes of curves in H_g and equivalence classes of Weierstrass equations in W_g, where $E,\bar{E}\in W_g$ are said to be equivalent over $\mathbb{F}$ if there exist such that the change of coordinates transforms (2.1) equation E to equation $\bar{E}$. Thus, it is enough to count the number of equivalence classes in W_g in order to count the number of isomorphism classes in H_g. In the remainder we call $E\in W_g$ a hyperelliptic curve and let isomorphism denote a change of coordinates of the above type.

3. Isomorphism classes of genus 2 hyperelliptic curves over $\mathbb{F}_q, q=2^n$

In this section, we count the exact number of isomorphism classes of genus 2 hyperelliptic curves over $\mathbb{F}_q, q=2^n$ and list all the representatives of each isomorphism class. From now on we let $q=2^n$.

Let E_1,E_2 be isomorphic curves of genus 2 defined over $\mathbb{F}_q$ given by the following equations;

$$E_1: y^2+(a_1x^2+a_3x+a_5)y=x^5+a_2x^4+a_6x^2+a_8x+a_{10}$$

$$E_2: y^2+(\bar{a_1}x^2+\bar{a_3}x+\bar{a_5})y=x^5+\bar{a_2}x^4+\bar{a_6}x^2+\bar{a_8}x+\bar{a_{10}}.$$

The equation E_1 can be transformed to the equation E_2 by changing of coordinates

$$\left\{\begin{array}{l} x\mapsto\alpha^2x+\beta \\ y\mapsto\alpha^5y+\alpha^4\gamma x^2+\alpha^2\delta x+\epsilon \end{array}\right\}$$

for some $\alpha \in \mathbb{F}_{2^n}^*, \beta, \gamma, \delta, \epsilon \in \mathbb{F}_{2^n}$([13]).
This gives the following relations;
(3.1)

$$\begin{cases} \alpha\bar{a_1} = a_1, \quad \alpha^3\bar{a_3} = a_3, \quad \alpha^5\bar{a_5} = \beta^2 a_1 + \beta a_3 + a_5 \\ \alpha^2\bar{a_2} = \beta + \gamma^2 + \gamma a_1 + a_2, \ \alpha^4\bar{a_4} = \delta a_1 + \gamma a_3 + a_4 \\ \alpha^6\bar{a_6} = \delta^2 + \beta^2\gamma a_1 + \epsilon a_1 + \beta\gamma a_3 + \delta a_3 + \beta a_4 + \gamma a_5 + a_6 \\ \alpha^8\bar{a_8} = \beta^4 + \beta^2\delta a_1 + \beta\delta a_3 + \epsilon a_3 + \beta^2 a_4 + \delta a_5 + a_8 \\ \alpha^{10}\bar{a_{10}} = \beta^5 + \epsilon^2 + \beta^2\epsilon a_1 + \beta^4 a_2 + \beta\epsilon a_3 + \beta^3 a_4 + \epsilon a_5 + \beta^2 a_6 + \beta a_8 + a_{10}. \end{cases}$$

Any hyperelliptic curve of genus 2 over $\mathbb{F}_{2^n}$ belongs to the exactly one of the following types and each isomorphism class of the curves should belong to the same type;

Type I : $a_1 \neq 0$ (also $\bar{a_1} \neq 0$),

Type II : $a_1 = 0,\ a_3 \neq 0$ (also $\bar{a_1} = 0,\ \bar{a_3} \neq 0$),

Type III : $a_1 = a_3 = 0,\ a_5 \neq 0$ (also $\bar{a_1} = \bar{a_3} = 0,\ \bar{a_5} \neq 0$).

We note above three types of curves should belong to different isomorphism classes from the relations in (3.1).

We summarize the elementary results on finite field $\mathbb{F}_q$ needed later.

Lemma 3.1. [12] *For $a \in \mathbb{F}_q$, the equation $x^2 + x = a$ has a solution in $\mathbb{F}_q$ if and only if $Tr(a) = 0$. Here, $Tr(\alpha) = \sum_{i=1}^{n} \alpha^{2^{i-1}}$ is a trace function.*

Corollary 3.2. [12] *For $a, b \in \mathbb{F}_q$, $a \neq 0$, the equation $x^2 + ax + b = 0$ has a solution in $\mathbb{F}_q$ if and only if $Tr(a^{-2}b) = 0$. If x_1 is one solution, then the other solution is $x_1 + a$.*

The following proposition states about the number of solutions of the polynomials.

Proposition 3.3. *Consider the following polynomial*

$$x^{16} + x + a = 0, \ \ a \in \mathbb{F}_{2^n}, a \neq 0. \tag{3.2}$$

(1) If n is odd, then (3.2) has either no solution or exactly two solutions and in this case, if x_1 is one solution, then the other solution is $x_1 + 1$.

(2) *If* $n \equiv 2 \pmod 4$, *then (3.2) has either no solution or exactly four solutions and in this case, if* x_1 *is one solution, then the others are* $x_1 + c, c \in \mathbb{F}_4^*$.

(3) *If* $n \equiv 0 \pmod 4$, *then (3.2) has* 16 *solutions if* $Tr_{\mathbb{F}_4}(a) = 0$, *and no solutions if* $Tr_{\mathbb{F}_4}(a) \neq 0$. *Here*

$$Tr_{\mathbb{F}_4}(\alpha) = \alpha + \alpha^{2^4} + \alpha^{2^8} + \cdots \alpha^{2^{n-4}}.$$

3.1. **Type I Curve.** In [5] it is shown that any hyperelliptic curve of Type I can be transformed in to the following form;

$$E_1 : y^2 + (x^2 + a_3 x + a_5)y = x^5 + a_8 x + a_{10}.$$

Let

$$E_2 : y^2 + (x^2 + \bar{a_3} x + \bar{a_5})y = x^5 + \bar{a_8} x + \bar{a_{10}}$$

be a hyperelliptic curve over $\mathbb{F}_q$ isomorphic to E_1. Then there exist $\beta, \gamma, \delta, \epsilon \in \mathbb{F}_q$, satisfying the equations;

$$\begin{cases} \beta = \gamma^2 + \gamma, \quad \delta = \gamma a_3, \quad \epsilon = \delta^2 + \beta^2\gamma + \beta\gamma a_3 + \delta a_3 + \gamma a_5 \\ \bar{a_3} = a_3, \quad \bar{a_5} = \beta^2 + \beta a_3 + a_5 \\ \bar{a_8} = \beta^4 + \beta^2\delta + \beta\delta a_3 + \epsilon a_3 + +\delta a_5 + a_8 \\ \bar{a_{10}} = \beta^5 + \epsilon^2 + \beta^2\epsilon + \beta\epsilon a_3 + \epsilon a_5 + \beta a_8 + a_{10}. \end{cases}$$

The above relations can be reduced the following equations;

(1) $\beta = \gamma^2 + \gamma$
(2) $\bar{a_3} = a_3$
(3) $\bar{a_5} = \beta^2 + \beta a_3 + a_5$
(4) $\bar{a_8} = \beta^4 + a_3^3\beta + a_8$
(5) $\bar{a_{10}} = a_3^4\beta^2 + a_3^3\beta^2 + a_3^2 a_5\beta + a_5^2\beta + a_8\beta + a_{10}$.

Now, we split the set of Type I curve into six disjoint unions;

$$A = \{y^2 + (x^2 + a_3 x + a_5)y = x^5 + a_8 x + a_{10} \mid a_i \in \mathbb{F}_{2^n}\}.$$

A can be splitted into the following six disjoint sets;

$$A = A_1 \cup B_1 \cup B_2 \cup B_3 \cup B_4 \cup C_1 \cup C_2,$$

where

$$A_1 = \{E \in A \,|\, a_3 = 0\},$$

$$B_1 = \{E \in A \,|\, a_3 \neq 0, Tr(a_3) = 0, Tr(a_3^{-2}a_5) = 0, a_8 = a_3^5 + a_3^4 + a_3^2a_5 + a_5^2\},$$
$$B_2 = \{E \in A \,|\, a_3 \neq 0, Tr(a_3) = 0, Tr(a_3^{-2}a_5) = 0, a_8 \neq a_3^5 + a_3^4 + a_3^2a_5 + a_5^2\},$$
$$B_3 = \{E \in A \,|\, a_3 \neq 0, Tr(a_3) = 0, Tr(a_3^{-2}a_5) \neq 0, a_8 = a_3^5 + a_3^4 + a_3^2a_5 + a_5^2\},$$
$$B_4 = \{E \in A \,|\, a_3 \neq 0, Tr(a_3) = 0, Tr(a_3^{-2}a_5) \neq 0, a_8 \neq a_3^5 + a_3^4 + a_3^2a_5 + a_5^2\},$$
$$C_1 = \{E \in A \,|\, a_3 \neq 0, Tr(a_3) \neq 0, Tr(a_3^{-2}a_5) = 0, \},$$
$$C_2 = \{E \in A \,|\, a_3 \neq 0, Tr(a_3) \neq 0, Tr(a_3^{-2}a_5) \neq 0, \}.$$

First, we count the exact number of singular curves which belong to each set.

Lemma 3.4. *Let*

$$V = \{E \in A \,|\, E \textit{ is singular}\}$$

and let $U_1 = V \cap A_1, V_i = V \cap B_i, i = 1, 2, 3, 4, W_j = V \cap C_j, j = 1, 2$. *Then* V *is the following disjoint union of sets;*

$$V = U_1 \cup V_1 \cup V_2 \cup V_3 \cup V_4 \cup W_1 \cup W_2.$$

Then $|U_1| = q^2,\ |V_1| = |V_3| = q(q-2)/4,\ |V_2| = q(q-1)(q-2)/2,\ |V_4| = 0,\ |W_1| = q^2(2q-1)/4,\ |W_2| = q^2/4$

(Proof) In [5] it was counted that $|V| = q^3$. More splitting is immediate from the direct counting and we omit the detailed proof. □

We now count number of isomorphism classes for each case;

About A_1; this is the case when $a_3 = 0$;
There exists a solution γ satisfying the equation (1) if and only if $Tr(\beta) = 0$. For each $E \in A_1$, there are $q/2$ curves isomorphic to E in A_1. Since there are $|U_1| = q^2$ many singular curves, we conclude that there are $(q^3 - q^2)/(q/2) = 2q(q-1)$ isomorphism classes.

About $B_i, i = 1, 2, 3, 4$; this is the case when $a_3 \neq 0$ and $Tr(a_3) = 0$;
First note that the equation (3) has a solution if and if $Tr(a_3^{-2}a_5) = Tr(a_3^{-2}\bar{a}_5)$. In this case, there are two distinct solutions, say $\{\beta_1, \beta_1 + a_3\}$. For each β, (1) has a solution if and only if $Tr(\beta) = 0$. Further, if β is a solution to (4), then so is $\beta + a_3$. On the other hand, if β is a solution to (5), then $\beta + a_3$ cannot be a solution unless $a_8 = a_3^5 + a_3^4 + a_3^2a_5 + a_5^2$.

(1) If $E_1, E_2 \in B_1$, then there are two different choices of β and four choice of γ satisfying all the equations from (1) to (5). For $E_1 \in A_1$, the number of curves isomorphic to E_1 is $q/4$. So the number of nonsingular isomorphism classes in B_1 is $|B_1 - V_1|/(q/4) = (q-1)(q-2)$.
(2) If $E_1, E_2 \in B_2$, then there are one choice of β and two choices of γ. So $|B_2 - V_2|/(q/2) = (q-1)(q-2)^2/2$.
(3) As the case B_1, if $E_1, E_2 \in B_3$, then there are two different choices of β and four choice of γ satisfying all the equation from (1) to (5). So $|B_3 - V_3|/(q/4) = (q-1)(q-2)$.
(4) If $E_1, E_2 \in B_4$, then there are one choice of β and and two choice of γ so isomorphism classes in B_4 is $|B_4 - V_4|/(q/2) = q(q-1)(q-2)/2$.

About $C_i, i = 1, 2$; this is the case when $a_3 \neq 0$ and $Tr(a_3) \neq 0$

(1) In this case $Tr(\beta) \neq Tr(\beta + a_3)$. So there is exactly one solution β of (3) whose corresponding equation (1) has two distinct solutions. So $|C_1 - W_1|/(q/2) = q(q-1)^2/2$.
(2) Since there is one solution β and two solution of γ as the case C_1, $|C_2 - W_2|/(q/2) = q(q^2-1)/2$.

If we summarize the above discussion, we get the following Theorem. Also, for each case Table shows how to select the representatives in each class;

Theorem 3.5. *(1) There are $(q-1)(2q^2+q-2)$ many isomorphic classes of genus 2 hyperelliptic curves of Type I over $\mathbb{F}_q$.*
(2) All the representatives from each class are given as

$$E : y^2 + (x^2 + a_3x + a_5)y = x^5 + a_8x + a_{10},$$

where a_i's can be chosen as the following Table;

a_3	a_5	a_8	a_{10}	*Number*
0	$\{0, \gamma_1\}$, $Tr(\gamma_1) = 1$	$a_8 \neq a_5^2$		$2q(q-1)$
$a_3 \neq 0$, $Tr(a_3) = 0$	$\{\gamma_2, \gamma_3\}$, $Tr(a_3^{-2}\gamma_2) = Tr(a_3^{-2}\gamma_3) = 0$ $\{x \mid x^2 + a_3x + \gamma_2 + \gamma_3 = 0, Tr(x) = 1\} \neq \phi$	[1]	[2]	$(q-1)(q-2)$
	γ_4 $Tr(a_3^{-2}\gamma_4) = 0$	[3]	[4]	$(q-1)(q-2)^2/2$
	$\{\gamma_5, \gamma_6\}$ $Tr(a_3^{-2}\gamma_5) = Tr(a_3^{-2}\gamma_6) = 1$, $\{x \mid x^2 + a_3x + \gamma_5 + \gamma_6 = 0, Tr(x) = 1\} \neq \phi$	[1]	[5]	$(q-1)(q-2)$
	γ_7 $Tr(a_3^{-2}\gamma_7) = 1$	[3]		$q(q-1)(q-2)/2$
$Tr(a_3) = 1$	0	[6]	[6]	$q(q-1)^2/2$
	γ_8 $Tr(a_3^{-2}\gamma_8) = 1$	[6]	[6]	$q(q^2-1)/2$

where

[1] $a_8 = a_3^5 + a_3^4 + a_3^2a_5 + a_5^2$
[2] If α *satisfies* $\alpha^2 + a_3\alpha + a_5 = 0$ *then* $a_{10} \neq (\alpha^8)(a_3^2)^{-1} + \alpha^5 + a_8\alpha + (a_8^2)(a_3^2)^{-1}$
[3] $a_8 \neq a_3^5 + a_3^4 + a_3^2a_5 + a_5^2$
[4] If α *is a solution of* $x^2+a_3x+a_5 = 0$ *then* $a_{10} \neq (\alpha^8)(a_3^2)^{-1}+\alpha^5+a_8\alpha+(a_8^2)(a_3^2)^{-1}$ *and* $a_{10} \neq (\alpha+a_3)^8(a_3^2)^{-1}+(\alpha+a_3)^5+a_8(\alpha+a_3)+(a_8^2)(a_3^2)^{-1}$
[5] $a_{10} \neq (a_8^2 + a_3^6a_5 + a_3^4a_5^2 + a_5^4 + a_3^5a_5)(a_3^2)^{-1}$
[6] $a_8 \neq a_3^5+a_3^4+a_3^2a_5+a_5^2$ *and* $a_{10} \neq (a_8^2+a_3^6a_5+a_3^4a_5^2+a_5^4+a_3^5a_5)(a_3^2)^{-1}$

Example 3.6. *The isomorphism classes of genus 2 hyperelliptic curves over* $\mathbb{F}_2$ *with Type I;*

No	*Representative* $E/\mathbb{F}_2$	$J_E(\mathbb{F}_2)$
1	$y^2 + x^2y = x^5 + x$	$\mathbb{Z}_8$
2	$y^2 + x^2y = x^5 + x + 1$	$\mathbb{Z}_4$
3	$y^2 + (x^2 + 1)y = x^5$	$\mathbb{Z}_{10}$
4	$y^2 + (x^2 + 1)y = x^5 + 1$	$\mathbb{Z}_2$
5	$y^2 + (x^2 + x)y = x^5 + 1$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$
6	$y^2 + (x^2 + x + 1)y = x^5 + 1$	$\mathbb{Z}_6$
7	$y^2 + (x^2 + x + 1)y = x^5 + x$	$\mathbb{Z}_{14}$
8	$y^2 + (x^2 + x + 1)y = x^5 + x + 1$	$\mathbb{Z}_2$

Genus 2 hyperelliptic curves over $\mathbb{F}_2$ with Type I

3.2. **Type II Curve.**

In Type II case the number of isomorphism classes of hyperelliptic curve of genus 2 has been explicitly counted[5]. Here we give a complete list of representatives of the curve of Type II case;

Theorem 3.7. [5]

(1) Every genus 2 hyperelliptic curve of Type II over $\mathbb{F}_q, q = 2^n$, can be represented by an equation of the form

$$E : y^2 + a_3xy = x^5 + a_4x^3 + a_6x^2 + a_{10},\ \ a_3 \neq 0.$$

(2) The number of isomorphism classes of genus-2 hyperelliptic curves of Type II over $\mathbb{F}_q$ is $2q(q-1)$.

Theorem 3.8. *(1) A set of representatives of the isomorphism classes of Type II is*

$$\{E : y^2{+}a_3xy = x^5{+}a_4x^3{+}a_6x^2{+}a_3^3|\ a_3, \gamma \in \mathbb{F}_q^*, a_6 \in \{0, \gamma\}, Tr(a_3^{-2}\gamma) = 1, a_4 \in \mathbb{F}_q\}$$

More explicitly, we have

(2) if n is odd, a set of representation of the isomorphism classes can be chosen as

$$\{y^2 + xy = x^5 + a_4x^3 + a_6x^2 + a_{10}|a_4, a_{10} \in \mathbb{F}_q, a_{10} \neq 0, a_6 \in \{0, 1\}\}.$$

(3) *If* $n \equiv 2 \pmod 4$, *we can write a set of representation of the isomorphism classes as*

$$\{y^2+a_3xy = x^5+a_4x^3+a_6x^2+1 \mid a_3, \gamma \in \mathbb{F}_q^*, a_6 \in \{0, \gamma\}, Tr(a_3^{-2}\gamma) = 1, a_4 \in \mathbb{F}_q\}.$$

Example 3.9. *The isomorphism classes over* $\mathbb{F}_2$ *with Type II;*

No	*Representative curve* $E/\mathbb{F}_2$	$J_E(\mathbb{F}_2)$
1	$y^2 + xy = x^5 + 1$	$\mathbb{Z}_8$
2	$y^2 + xy = x^5 + x^2 + 1$	$\mathbb{Z}_2$
3	$y^2 + xy = x^5 + x^3 + 1$	$\mathbb{Z}_4$
4	$y^2 + xy = x^5 + x^3 + x^2 + 1$	$\mathbb{Z}_{10}$

Genus-2 hyperelliptic curves over $\mathbb{F}_2$ with Type II

3.3. **Type III Curve.**

In this section, we count the exact number of isomorphism class and list all the representatives of each isomorphism classes of Type III in the case of $a_4 = 0$. The problem remains still open when $a_4 \neq 0$.

Before we state theorem we remark supersingular property;

Remark 3.10. (1) *Any hyperelliptic curve of genus* g *in characteristic two of the form* $y^2 + h(x)y = f(x)$ *with* $1 \leq deg(h(x)) \leq g + 1$ *cannot be supersingular* [7]. *Therefore, the curves of Type I, II are nonsupersingular.*

(2) *The genus* 2 *hyperelliptic curves over* $\mathbb{F}_q$ *of the form* $y^2 + cy = f(x)$ *where* $f(x)$ *is monic of degree* 5 *and* $c \in \mathbb{F}_q^*$ *are supersingular* [7]. *Therefore the curves of Type III are supersingular.*

Every genus 2 hyperelliptic curve of Type III over $\mathbb{F}_q, q = 2^n$, can be represented by the equation of the form [5]

$$E : y^2 + a_5y = x^5 + a_4x^3 + a_8x + a_{10},\ a_5 \neq 0.$$

From now on we assume $a_4 = 0$. The following three different cases are considered;

Case when $n \equiv 1 \pmod 2$, $n \equiv 2 \pmod 4$, $n \equiv 0 \pmod 4$.

3.3.1. **Case when** $n \equiv 1 \pmod 2$. since n is odd, $g.c.d\,(2^n-1,5)=1$. Hence $\mathbb{F}_q^*$ has no elements of order 5. Let $E'/\mathbb{F}_q$ be the curve given by the equation

$$E' : y^2 + a_5' y = x^5 + a_8' x + a_{10}', \quad a_5' \neq 0.$$

Let $r = \sqrt[5]{a_5'}$. Then the admissible change of variables $(x,y) \to (r^2x, r^5y)$ transforms E' to a curve given by

$$E : y^2 + y = x^5 + a_8 x + a_{10}. \tag{3.3}$$

So there are q^2 many hyperelliptic curves has the form (3.3). Let $\bar{E}$ be the curve given by

$$\bar{E} : y^2 + y = x^5 + \bar{a_8} x + \bar{a_{10}}$$

isomorphic to E. Then there exist $\alpha, \gamma, \epsilon \in \mathbb{F}_q$ such that

$$\begin{cases} \alpha^5 = 1, \quad \alpha^{16}\bar{a_8}^2 = \gamma^{16} + a_8^2 + \gamma a_5^3 \\ \alpha^{10}\bar{a_{10}} = \gamma^{10} + \epsilon^2 + \epsilon a_5 + \gamma^2 a_8 + a_{10}. \end{cases} \tag{3.4}$$

Since $\mathbb{F}_q$ has no elements of order 5, $\alpha = 1$.

We now claim that any hypereilltic curve E of the form (3.3) is isomorphic to one of the following three,

$$E_1;\ y^2 + y = x^5, \quad E_2;\ y^2 + y = x^5 + x, \quad E_3; y^2 + y = x^5 + x + 1;$$

(A) Suppose that $E \cong E_1$ over $\mathbb{F}_q$. Then, from (3.4) there exists $\gamma, \epsilon \in \mathbb{F}_q$, satisfying the equation;

(6) $\gamma^{16} + \gamma + a_8^2 = 0$
(7) $\epsilon^2 + \epsilon + \gamma^{10} + a_8\gamma^2 + a_{10} = 0.$

Since n is odd, Proposition 3.3 implies that (6) has two distinct solutions, namely, $\{\gamma_1, \gamma_1 + 1\}$. Note that (7) has two distinct solution ϵ for only exactly one $\gamma \in \{\gamma_1, \gamma_1 + 1\}$ with $Tr(\gamma) = 0$ since n is odd. As a conclusion there exist only two solutions (γ, ϵ) satisfying (6) and (7). This implies that there are $q^2/2$ curves isomorphic to E_1.

(B) Suppose that $E \cong E_2$. First check that $E_1 \not\cong E_2$ over $\mathbb{F}_q$, because the equation (6) has no solution in $\mathbb{F}_q$. Now, the relation (3.4) implies that there exists $\gamma, \epsilon \in \mathbb{F}_q$, satisfying

(8) $\gamma^{16} + \gamma + 1 + a_8^2 = 0$
(9) $\epsilon^2 + \epsilon + \gamma^{10} + a_8\gamma^2 + a_{10} = 0.$

Here (8) has two solutions $\gamma_1, \gamma_1 + 1$. For each γ, there are two solutions to (9). Thus there are four solutions satisfying (8) and (9) and $q^2/4$ curves isomorphic to E_2.

(C) First note that $E_1 \not\cong E_3$ and $E_2 \not\cong E_3$. are $q^2/4$ curves isomorphic to E_3 by the similar manner to the case (B).

Theorem 3.11. *Let $q = 2^n, n$ odd. Then there are three isomorphism classes and the representatives of each class are*

(1) $y^2 + y = x^5$
(2) $y^2 + y = x^5 + x$
(3) $y^2 + y = x^5 + x + 1.$

3.3.2. **Case II** $n \equiv 2 \pmod 4$. since $n \equiv 2 \pmod 4$, $\mathbb{F}_q^*$ has no elements of order 5. So we can assume the hyperellipctic curve has the following form as the Case I.

$$E : y^2 + y = x^5 + a_8 x + a_{10}.$$

Assume that

$$\bar{E} : y^2 + y = x^5 + \bar{a_8} x + \bar{a_{10}}$$

be isomorphic to E. Then there exist $\gamma, \epsilon \in \mathbb{F}_q$ such that

(10) $\gamma^{16} + \gamma + a_8^2 + \bar{a_8}^2 = 0$
(11) $\epsilon^2 + \epsilon + \gamma^{10} + a_8\gamma^2 + a_{10} + \bar{a_{10}} = 0.$

If γ_1 is a solution of (10), so are $\gamma_1 + 1, \gamma_1 + c_1$ and $\gamma_1 + c_2$ with $\mathbb{F}_4 = \{0, 1, c_1, c_2\}$ by Proposition 3.3(2). For γ_1, if (11) has a solution ϵ, then $Tr(\gamma_1^{10} + a_8\gamma_1^2 + a_{10} + \bar{a_{10}}) = 0$,

$$Tr((\gamma_1 + 1)^{10} + a_8(\gamma_1 + 1)^2 + a_{10} + \bar{a_{10}}) = Tr(a_8),$$

$$Tr((\gamma_1 + c_1)^{10} + a_8(\gamma_1 + c_1)^2 + a_{10} + \bar{a_{10}}) = 1 + Tr(c_1 a_8) + Tr(a_8),$$

$$Tr((\gamma_1 + c_2)^{10} + a_8(\gamma_1 + c_2)^2 + a_{10} + \bar{a_{10}}) = 1 + Tr(c_1 a_8).$$

There are 8 solutions satisfying (10) and (11) if $Tr(a_8) = 0$ and $Tr(c_1 a_8) = 1$. Otherwise there are 4 solutions. Since there are $q/4$ elements a_8 in $\mathbb{F}_q$ satisfying $Tr(a_8) = 0$ and $Tr(c_1 a_8) = 1$ and $q^2/8$ curves isomorphic to E, there are 2 isomorphism classes. For the other cases, there are one isomorphism class. We summarize the result as following;

Theorem 3.12. *Let* $n \equiv 2 \pmod 4$. *Then there are 5 isomorphism classes and the representatives of each class are*

(1) $y^2 + y = x^5$
(2) $y^2 + y = x^5 + x$
(3) $y^2 + y = x^5 + x + \gamma, Tr(\gamma) = 1$
(4) $y^2 + y = x^5 + c_1 x$
(5) $y^2 + y = x^5 + c_2 x.$

3.3.3. **Case III.** $n \equiv 0 \pmod 4$. let E be the Type III curve given by

$$E : y^2 + a_5 y = x^5 + a_8 x + a_{10}, \quad a_5 \neq 0.$$

In this case, we split the cases into three distinct cases;
Type III-1; $\sqrt[5]{a_5} \notin \mathbb{F}_q$
Type III-2 ; $\sqrt[5]{a_5} \in \mathbb{F}_q$ and $Tr_{\mathbb{F}_4}(a_8) \neq 0$
Type III-3; $\sqrt[5]{a_5} \in \mathbb{F}_q$ and $Tr_{\mathbb{F}_4}(a_8) = 0$

(1) **Type III-1 Curves**
Let E_1, E_2 be isomorphic to each other given by the following equations;

$$E_1 : y^2 + a_5 y = x^5 + a_{10},$$

$$E_2 : y^2 + \bar{a_5} y = x^5 + \bar{a_8} x + \bar{a_{10}}.$$

Then there exist $\alpha, \gamma, \epsilon \in \mathbb{F}_q$, satisfying the equations

(12) $\alpha^5 = a_5/\bar{a_5}$
(13) $\gamma^{16} + a_5^3 \gamma + \alpha^{16} \bar{a_8}^2 = 0$
(14) $\epsilon^2 + a_5 \epsilon + \gamma^{10} + a_8 \gamma^2 + a_{10} + \alpha^{10} \bar{a_{10}} = 0.$

Since $\bar{a_5} = a_5/\alpha^5$ and $\sqrt[5]{a_5} \notin \mathbb{F}_q$, also $\sqrt[5]{\bar{a_5}} \notin \mathbb{F}_q$. Hence E_2 is a Type III-1 curve. Note that (12) has exactly 5 solutions, namely $u_i\alpha_1$ where $u_i^5 = 1, 0 \le i \le 4, u_0 = 1$. Since $\sqrt[5]{a_5} \notin \mathbb{F}_q$, (13) has exactly one solution for each α. For $\alpha = u_i\alpha_1, 0 \le i \le 4$, these unique solutions to (13) are $\gamma = u_i\gamma_1,\ 0 \le i \le 4$ respectively. For $(\alpha,\gamma) = (u_i\alpha_1, u_i\gamma_1), 0 \le i \le 4$, there are 2 solutions to (14), namely $\epsilon_1, \epsilon_1 + a_5$. Thus there are 10 admissible change of variables which transform E_1 to E_2. Since the number of curves isomorphic to E_1 is $(q-1)q^2/10$ and Type III-1 curves is $4(q-1)q^2/5$, there are 8 isomorphism classes.

(2) **Type III-2 Curves**

Since $\sqrt[5]{a_5} \in \mathbb{F}_q$, we can transform any Type III-2 (and Type III-3) curves to the form $y^2+y = x^5+a_8x+a_{10}$. Let E_1, E_2 be the isomorphic Type III-2 curves given by

$$E_1 : y^2 + y = x^5 + a_8x,\ \ Tr_{\mathbb{F}_4}(a_8) = 1,$$

$$E_2 : y^2 + y = x^5 + \bar{a_8}x + \bar{a_{10}}.$$

Then there exists $\alpha_1, \gamma_1, \epsilon_1 \in \mathbb{F}_q$, satisfying

(15) $\alpha^5 = 1$
(16) $\gamma^{16} + \gamma + a_8^2 + \alpha\bar{a_8}^2 = 0$
(17) $\epsilon^2 + \epsilon + \gamma^{10} + a_8\gamma^2 + \bar{a_{10}} = 0$

Since $Tr_{\mathbb{F}_4}(a^{2^4}) = a$ for all $a \in \mathbb{F}_q$,

$$Tr_{\mathbb{F}_4}(\bar{a_8}^2)\ \ = Tr_{\mathbb{F}_4}(\frac{\gamma^{16}}{\alpha^{16}}) + Tr_{\mathbb{F}_4}(\frac{\gamma}{\alpha}) + Tr_{\mathbb{F}_4}(\frac{a_8^2}{\alpha}) = Tr_{\mathbb{F}_4}(\frac{a_8^2}{\alpha}).$$

If $\alpha = 1, u_1, u_2, u_3$ or u_4, then $Tr_{\mathbb{F}_4}(a_8/\alpha) = 1, u_4, u_3, u_2$ or u_1 respectively. Thus $Tr_{\mathbb{F}_4}(\bar{a_8}) \ne 0$, and E_2 is also a Type III-2 curve. For each choice of α, equation (16) has exactly 16 solutions or no solution, according to whether $Tr_{\mathbb{F}_4}(a_8^2 + \alpha\bar{a_8}^2) = 0$ or not respectively. Assume that without loss of generality $Tr_{\mathbb{F}_4}(\bar{a_8}^2) = 1$. Then the equation (16) has 16 distinct solutions,$\gamma_1 + w, w \in \mathbb{F}_{16}$. One can check (17) has solutions for half of elements w in $\mathbb{F}_{16}$. Thus there are 16 solutions (α,γ,ϵ) to the equations $(15), (16), (17)$. Now there are $5q^2/16$ Type

III-2 curves isomorphic to E_1. Since the number of Type III-2 curves is $15q^2/16$, we conclude that the Type III-2 curves form 3 isomorphism classes.

(3) **Type III-3 Curves**
Let E_1 be the Type III-3 curve given by the equation

$$E_1 : y^2 + y = x^5$$

and let

$$E_2 : y^2 + y = x^5 + \bar{a_8}x + \bar{a_{10}}$$

be a curve over $\mathbb{F}_q$ isomorphic to E_1. Since $E_1 \cong E_2$ over $\mathbb{F}_q$, there exists $\alpha_1, \gamma_1, \epsilon_1 \in \mathbb{F}_q$, satisfying

(18) $\alpha^5 = 1$
(19) $\gamma^{16} + \gamma + \alpha\bar{a_8}^2 = 0$
(20) $\epsilon^2 + \epsilon + \gamma^{10} + \bar{a_{10}} = 0.$

Note that

$$Tr_{\mathbb{F}_4}(\bar{a_8}^2) = Tr_{\mathbb{F}_4}(\frac{\gamma^{16}+\gamma}{\alpha}) = Tr_{\mathbb{F}_4}(\frac{\gamma^{16}}{\alpha^{16}}) + Tr_{\mathbb{F}_4}(\frac{\gamma}{\alpha}) = 0.$$

Since $\alpha^5 = 1$, we have $\alpha = 1, u_1, u_2, u_3$ or u_4. Because $Tr_{\mathbb{F}_4}(\bar{a_8}) = 0$, we have $Tr_{\mathbb{F}_4}(u_i\bar{a_8}) = 0$ for $i = 1, 2, 3, 4$. Thus for each choice of α the equation (19) has 16 solutions in $\mathbb{F}_q$. And for each solution γ to (19), (20) has solutions in $\mathbb{F}_q$. So there are 160 solutions $(\alpha, \gamma, \epsilon)$ of the equations (18), (19) and (20). Since there are $5q^2$ admissible changes of variables, there are $5q^2/32$ Type III-3 curves isomorphic to E_1, and these account for half of the $q^2/16$ Type III-3 curves.

So, we summarize the above results to the following table;

Theorem 3.13. *Let* $q = 2^n, n \equiv 0 \pmod 4$. *There are* 13 *isomorphism classes and the representatives are the following table; where* $\alpha, \beta_i, \gamma_j, \delta \in \mathbb{F}_q$, $\sqrt[5]{\alpha} \notin \mathbb{F}_q$ *and* $\mathbb{F}_4 = \{0, 1, c_1, c_2\}$.

No	*Representative*		*Type*
1	$y^2+\alpha y=x^5$		$III-1$
2	$y^2+\alpha y=x^5+\beta_1$	$Tr(\alpha^{-2}\beta_1)=1$	$III-1$
3	$y^2+\alpha^2 y=x^5$		$III-1$
4	$y^2+\alpha^2 y=x^5+\beta_2$	$Tr(\alpha^{-4}\beta_2)=1$	$III-1$
5	$y^2+\alpha^3 y=x^5$		$III-1$
6	$y^2+\alpha^3 y=x^5+\beta_3$	$Tr(\alpha^{-6}\beta_3)=1$	$III-1$
7	$y^2+\alpha^4 y=x^5$		$III-1$
8	$y^2+\alpha^4 y=x^5+\beta_4$	$Tr(\alpha^{-8}\beta_4)=1$	$III-1$
9	$y^2+y=x^5+\gamma_1 x$	$Tr_4(\gamma_1)=1$	$III-2$
10	$y^2+y=x^5+\gamma_2 x$	$Tr_4(\gamma_2)=c_1$	$III-2$
11	$y^2+y=x^5+\gamma_3 x$	$Tr_4(\gamma_3)=c_2$	$III-2$
12	$y^2+y=x^5$		$III-3$
13	$y^2+y=x^5+\delta$	$Tr(\delta)=1$	$III-3$

Example 3.14. *The isomorphism classes of genus* 2 *hyperelliptic curves over* $\mathbb{F}_{2^4}$ *with Type III ;*

For $F_{2^4}=F_2[w]/<w^4+w+1>$

No	*Representative curve* $E/\mathbb{F}_{2^4}$	*Type*
1	$y^2+w^3y=x^5$	$TypeIII-1$
2	$y^2+w^3y=x^5+1$	$TypeIII-1$
3	$y^2+(w^3+w^2)y=x^5$	$TypeIII-1$
4	$y^2+(w^3+w^2)y=x^5+\beta_2$	$TypeIII-1$
5	$y^2+(w^3+w)y=x^5$	$TypeIII-1$
6	$y^2+(w^3+w)y=x^5+1$	$TypeIII-1$
7	$y^2+(w^3+w^2+w+1)y=x^5$	$TypeIII-1$
8	$y^2+(w^3+w^2+w+1)y=x^5+1$	$TypeIII-1$
9	$y^2+y=x^5+x$	$TypeIII-2$
10	$y^2+y=x^5+(w^2+w)x$	$TypeIII-2$
11	$y^2+y=x^5+(w^2+w+1)x$	$TypeIII-2$
12	$y^2+y=x^5$	$TypeIII-3$
13	$y^2+y=x^5+w^3$	$TypeIII-3$

4. Conclusion

It may be useful to classify the isomorphism classes of hyperelliptic curves of small genus over finite fields. In this paper we study hyperelliptic Weierstrass equations and count the exact number of isomorphism, which preserves infinity, classes and list all the representatives of isomorphism classes with some exception for Type III case. Note that the above isomorphism classifies the hyperelliptic curves as projective varieties. So it will be important to give further identification of their Jacobians.

References

[1] L. M. Adleman, *A subexponential Algorithm for the discrete logarithm problem with applications to cryptography* , Proc. 20th IEEE Found. Comp. Sci. Symp., 55-60, 1979.

[2] L. Adleman, J. Demarrais and M.Huang, A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians fo large genus hyperelliptic curves over finite fields, Algorithmic Number Theory, LNCS 877(1994), 28-40, Springer-Verlag, Berlin.

[3] E. Arabello, et al., *Geometry of algebraic curves*, Grundlehren Math. Wiss. 267, Springer-Verlag, New York, 1985.

[4] G. Cardona and E. Nart, *Curves of genus two over fields of even characteristic*,

[5] Y. Choie and D. Yun, *Isomosrphism classes of Hyperelliptic curves of genus 2 over F_q* ACISP'02,pp.190-202 (2002) LNCS, Springer Verlag.

[6] G.Frey and H.-G. Rúck, *A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves*, Math. Comp., 62, 865-874, 1994.

[7] S. Galbraith, Supersingular curves in Cryptography, in C. Boyd (ed.) ASIACRYPT 2001, Springer LNCS 2248 (2001) 495–513.

[8] P. Gaudry, *A variant of the Adleman-DeMarrais-Huang algorithm and its application to small genera* , In Advances in Cryptology, EUROCRYPT 2000, Springer-Verlag LNCS 1807, 19-34, 2000.

[9] L. Hernández Encinas, A. J. Menezes, and J. Muñoz Masqué, *Isomorphism classes of genus-2 hyperelliptic curves over finite fields* , Applicable Algebra in Engineering, Communication and Computing, Volume 13 Issue 1 (2002) pp 57-65.

[10] N. Koblitz, *Elliptic curve cryptosystems*, Math. of Comp. vol 48, 203-209, 1987.

[11] N. Koblitz, *Hyperelliptic cryptosystems*, J. Crypto., 1,139-150, 203-209, 1989.

[12] R. Lidi and H. Niederreiter, *Finite fields, Encyclopedia of Math. and its application*, Vol. 20, Addison-Wesley, 1983.

[13] P. Lockhart, *On the discriminant of a hyperelliptic curve*, Trans. Amer. Math. Soc. 342, 2, 729-752, 1994.

[14] A. Menezes and N. Koblitz, *Elliptic curve public key cryptosystems* , Kluwer Academic Publishers, 1993.

[15] V. Miller, *Uses of elliptic curves in cryptography* , Advances in cryptology - Crypto '85, LNCS 218, 417-426, 1986.

[16] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.