JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume 15, No. 2, December 2002

ISOMORPHISM CLASSES OF HYPERELLIPTIC CURVES OF GENUS 2 OVER F_{2^n}

Chun Soo Choi* and Min Surp Rhee**

Abstract. L. H. Encinas, A. J. Menezes, and J. M. Masque in [2] proposed a classification of isomorphism classes of hyperelliptic curve of genus 2 over finite fields with characteristic different from 2 and 5. Y. Choie and D. Yun in [1] obtained for the number of isomorphic classes of hyperelliptic curves of genus 2 over F_q using direct counting method. In this paper we will classify the isomorphism classes of hyperelliptic curves of genus 2 over F_{2^n} for odd n, represented by an equation of the form $y^2 + a_5 y = x^5 + a_8 x + a_{10} (a_5 \neq 0)$.

1. Introduction

In 1989, N. Koblitz generalized the concept of elliptic curve[3]. In [2], L. H Encinas, A. J. Menezes, and J. M. Masque proposed a classification of isomorphism classes of genus 2 hyperelliptic curve over finite fields with characteristic different from 2 and 5. Y. Choie and D. Yun in [1] obtained some bounds for the number of isomorphic classes of hyperelliptic curves of genus 2 over F_q. Also, they obtained for the number of isomorphic classes of hyperelliptic curves of genus 2 over F_q using direct counting method.

In this paper we will classify the isomorphism classes of hyperelliptic curves of genus 2 over a finite field F_{2^n} with characteristic 2 for odd n, represented by an equation of the form

$$y^2 + a_5 y = x^5 + a_8 x + a_{10} (a_5 \neq 0).$$

Received by the editors on January 25, 2003.
2000 *Mathematics Subject Classifications*: 14H45, 94A60.
Key words and phrases: trace, ordered basis, hyperelliptic curve of genus 2, isomorphism class.

In Chapter 2, we introduce some definitions and some properties which will be used in this paper. In Chapter 3, we prove our main theorems for isomorphism classes of hyperelliptic curves of genus 2 over F_{2^n}.

2. Preliminaries

Let F_{q^n} be an extension field of the Galois field F_q with q elements. Then the map $Tr_{F_q} : F_{q^n} \to F_q$ defined by

$$Tr_{F_q}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}} (\alpha \in F_{q^n})$$

is called a trace function and the image $Tr_{F_q}(\alpha)$ of α is called the trace of α. In other words, the trace of α over F_q is the sum of the conjugates of α with respect to F_q. In particular, we simply write Tr for Tr_{F_2}. For $\alpha, \beta \in F_{q^n}$ and $c \in F_q$, the trace function have the following properties:

(1) $Tr_{F_q}(\alpha + \beta) = Tr_{F_q}(\alpha) + Tr_{F_q}(\beta)$.
(2) $Tr_{F_q}(c\alpha) = cTr_{F_q}(\alpha)$.
(3) $Tr_{F_q}(c) = nc$.
(4) $Tr_{F_q}(\alpha) = Tr_{F_q}(\alpha^q)$.

It is well known that $Tr(\alpha) = 0$ if and only if $\alpha = \beta^2 + \beta$ for some $\beta \in F_{2^n}$[3]. Also, a trinomial of the form $x^2 + \alpha x + \beta = 0$ has a root in F_{q^n} if and only if $Tr(\alpha^{-2}\beta) = 0$[3].

Now, we consider the roots of $x^{2^m} + ax + b = 0$ $(a, b \in F_{2^n})$ as follows.

Proposition 2.1 Let $Z(L)$ and $Z(P)$ be the sets of all roots of $x^{2^m} + x = 0$ and $x^{2^m} + x = b$ $(b \in F_{2^n})$, respectively. Then $Z(L) = F_{2^d}$, where $F_{2^d} \subseteq F_{2^n}$ and $d = (n, m)$. The equation $x^{2^m} + x + b = 0$ has a root x_0 for some x_0 in F_{2^n} if and only if $Tr_{F_{2^d}}(b) = \sum_{i=0}^{k-1} b^{2^{im}} = 0$, where $k = \frac{n}{d}$. Moreover, If $x^{2^m} + x + b = 0$ has a root x_0 in F_{2^n}, then $Z(P) = x_0 + Z(L)$.

Proof. The proof follows from [7].

Hence we have the following proposition from Proposition 2.1.

Proposition 2.2 Let

$$x^{16} + ax + b = 0 \tag{2.1}$$

be an equation over F_{2^n}, where $a \neq 0$. Then :

(1) If n is odd, then (2.1) has 2 roots if and only if $Tr_{F_q}(\frac{b}{\sqrt[15]{a^{16}}}) = 0$

(2) If n is even, then (2.1) has q roots if and only if $\sqrt[15]{a} \in F_{2^n}$ and $Tr_{F_q}(\frac{b}{\sqrt[15]{a^{16}}}) = 0$, where $q = 2^{(4,n)}$.

Proof. (1) Suppose that n is odd. Then $(4, n) = 1$ and by Proposition 2.1 $Z(L) = F_2$. Since n is odd, $gcd(2^n - 1, 3) = 1$ and $gcd(2^n - 1, 5) = 1$. Note $F_{2^n} - \{0\}$ is a finite cyclic group of order $2^n - 1$, which is relatively prime to 15. Hence we have $\{s^{15} | s \in F_{2^n}\} = F_{2^n}$ and so $\sqrt[15]{a} \in F_{2^n}$ for every $a \in F_{2^n}$. Then the equation (2.1) would be

$$x^{16} + x + \frac{b}{\sqrt[15]{a^{16}}} = 0.$$

Thus (1) holds by Propositon 2.1.

(2) Assume that n is even and $\sqrt[15]{a} \in F_{2^n}$. Then the equation (2.1) would be

$$x^{16} + x + \frac{b}{\sqrt[15]{a^{16}}} = 0.$$

Hence by Proposition 2.1, $x^{16} + x + \frac{b}{\sqrt[15]{a^{16}}} = 0$ has q roots in F_{2^n} if and only if $Tr_{F_q}(\frac{b}{\sqrt[15]{a^{16}}}) = 0$ where $q = 2^{(4,n)}$. Thus (2) holds.

The following concepts are very useful to find the trace of an element.

Definition 2.3 Two ordered bases $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ and $\{\beta_1, \beta_2, \cdots,$

$\beta_n\}$ of F_{2^n} over F_2 are said to be dual if $Tr(\alpha_i\beta_j) = \delta_{ij}$, where $\delta_{ij} = \begin{cases} 0 & for\ i \neq j \\ 1 & for\ i = j \end{cases}$.

When we represent x by a basis and y by its dual basis for any $x, y \in F_{2^n}$, it follows from the above definition that $Tr(xy) = x \cdot y$. Throughout this paper, whenever we use the notation $x \cdot y$ for $x, y \in F_{2^n}$, we assume x, y are represented by a basis and its dual basis, respectively.

Let C be the equation over F_{2^n} given by $y^2 + H(x)y = F(x)$ where $H(x)$ and $F(x)$ are polynomials over F_{2^n}. A point (x, y) on C is said to be singular if x and y are in the algebraic closure of F_{2^n} which satisfies the equations $H(x) = 0$ and $H'(x)y + F'(x) = 0$, where $H'(x)$ and $F'(x)$ are the formal derivative of $H(x)$ and $F(x)$, respectively.

Definition 2.4 A hyperelliptic curve C of genus g over F_{2^n} $(g \geq 1)$ is an equation of the form

$$C : y^2 + H(x)y = F(x)$$

which has no singular points on C, where $H(x)$ is a polynomial of degree at most g and $F(x)$ is a monic polynomial of degree $2g + 1$.

A point $(x, y) \in F_{2^n} \times F_{2^n}$ on the curve C is said to be an F_{2^n}-rational point on C. Then the set of all F_{2^n}-rational points on C, denoted by $C(F_{2^n})$, is defined by

$$C(F_{2^n}) = \{(x, y) \in F_{2^n} \times F_{2^n} | y^2 + H(x)y = F(x)\} \cup \{\ \mathrm{O}\}$$

where O is the ideal point which makes $C(F_{2^n})$ an additive group[6]. The proof of following properties is trivial.

Now, we briefly explain projective varieties and Weierstrass equations. Their concepts are taken from [6]. Two hyperelliptic curves are said to be isomorphic over F_{2^n} if they are isomorphic as projective varieties over F_{2^n}. Briefly, two projective varieties V_1 and V_2 over F_{2^n} are isomorphic over F_{2^n} if there exist morphisms $\phi : V_1 \to V_2$ and $\psi : V_2 \to V_1$ (ϕ, ψ are defined over F_{2^n}) such that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity maps on V_1 and V_2, respectively. Let $H(x)$ and $F(x)$ are polynomials over F_{2^n}. An equation H over F_{2^n} of the form

$$H : y^2 + H(x)y = F(x)$$

is said to be a Weierstrass equation of genus g over F_{2^n} if $deg(H(x)) \leq g$, $deg(F(x)) = 2g+1$, $F(x)$ is monic and there are no singular points. Two Weierstrass equations H and H' are said to be equivalent over F_{2^n} if there exist α and β in F_{2^n} with $\alpha \neq 0$, and a polynomial $T(x)$ over F_{2^n} with $deg(T(x)) \leq g$, such that the change of coordinates

$$(x, y) \to (\alpha^2 x + \beta, \alpha^{2g+1} y + T(x))$$

transforms equation H to equation H'.

Let's denote by H_g and M_g the set of all hyperelliptic curves of genus g over F_{2^n} and the set of all Weierstrass equations of genus g over F_{2^n}, respectively. The following proposition explains the relation between isomorphism classes of hyperelliptic curves in H_g and equivalence classes of Weierstrass equations in M_g.

Proposition 2.5 There is a 1-1 correspondence between isomorphism classes of hyperelliptic curves in H_g and equivalence classes of Weierstrass equations in M_g.

Proof. The proof follows from [2].

Now, assume that $g = 2$, so $F(x) = x^5 + a_2x^4 + a_4x^3 + a_6x^2 + a_8x + a_{10}$ and $H(x) = a_1x^2 + a_3x + a_5$ where $a_i \in F_{2^n}$. Then we can get the following.

Proposition 2.6 Let E_1 and E_2 be two hyperelliptic curves of genus 2 over F_{2^n} given by

$$E_1 : y^2 + (a_1x^2 + a_3x + a_5)y = x^5 + a_2x^4 + a_4x^3 + a_6x^2 + a_8x + a_{10}$$

$$E_2 : y^2 + (\bar{a_1}x^2 + \bar{a_3}x + \bar{a_5})y = x^5 + \bar{a_2}x^4 + \bar{a_4}x^3 + \bar{a_6}x^2 + \bar{a_8}x + \bar{a_{10}}.$$

Then E_1 and E_2 are isomorphic over F_{2^n}, denoted by $E_1 \cong E_2$, if and only if there exist $\alpha(\neq 0)$, β, γ, δ and ϵ in F_{2^n} such that the change of variables

$$(x, y) \to (\alpha^2x + \beta, \alpha^5y + \alpha^4\gamma x^2 + \alpha^2\delta x + \epsilon) \tag{2.2}$$

transforms E_1 to E_2. In this case we have the following equations (2.3) :

$$\begin{cases} \alpha\bar{a_1} = a_1 \\ \alpha^3\bar{a_3} = a_3 \\ \alpha^5\bar{a_5} = a_5 + \beta a_3 + \beta^3 a_1 \\ \alpha^2\bar{a_2} = a_2 + \gamma a_1 + \gamma^2 + \beta \\ \alpha^4\bar{a_4} = a_4 + \gamma a_3 + \delta a_1 \\ \alpha^6\bar{a_6} = a_6 + \gamma a_5 + \beta a_4 + (\delta + \beta\gamma)a_3 + (\epsilon + \beta^2\gamma)a_1 + \delta^2 \\ \alpha^8\bar{a_8} = a_8 + \delta a_5 + \beta^2 a_4 + (\epsilon + \beta\delta)a_3 + \beta^2\delta a_1 + \beta^4 \\ \alpha^{10}\bar{a_{10}} = a_{10} + \beta a_8 + \beta^2 a_6 + \epsilon a_5 + \beta^3 a_4 + \beta\epsilon a_3 + \beta^4 a_2 \\ \qquad\qquad + \beta^2\epsilon a_1 + \epsilon^2 + \beta^5 \end{cases} \tag{2.3}$$

Proof The proof may be found in [2].

First of all, we explain the isomorphism classes of hyperelliptic curves of genus 2 over F_{2^n}, represented by an equation of the form

$$y^2 + a_5 y = x^5 + a_2 x^4 + a_4 x^3 + a_6 x^2 + a_8 x + a_{10} (a_5 \neq 0)$$

Proposition 2.7[1] Let E_1 and E_2 be two hyperelliptic curves of genus 2 over F_{2^n} given by

$$E_1 : y^2 + a_5 y = x^5 + a_2 x^4 + a_4 x^3 + a_6 x^2 + a_8 x + a_{10} (a_5 \neq 0)$$

$$E_2 : y^2 + \bar{a_5} y = x^5 + \bar{a_4} x^3 + \bar{a_8} x + \bar{a_{10}} (\bar{a_5} \neq 0).$$

Then E_1 is isomorphic to E_2.

Proof Suppose that E_1 is a hyperelliptic curve of genus 2 over F_{2^n} given by an equation of the form

$$E_1 : y^2 + a_5 y = x^5 + a_2 x^4 + a_4 x^3 + a_6 x^2 + a_8 x + a_{10} (a_5 \neq 0).$$

Then E_1 is transformed into E_2 given by an equation of the form

$$E_2 : y^2 + \bar{a_5} y = x^5 + \bar{a_4} x^3 + \bar{a_8} x + \bar{a_{10}} (\bar{a_5} \neq 0)$$

by the change of variables

$$(x, y) \rightarrow (\alpha^2 x + \beta, \alpha^5 y + \alpha^4 \gamma x^2 + \alpha^2 \delta x + \epsilon)$$

where $\beta = \gamma^2 + a_2$ and $\delta^2 = \beta a_4 + \gamma a_5 + a_6$.

From Proposition 2.7, every hyperelliptic curve of genus 2 over F_{2^n} given by an equation of the form

$$y^2 + a_5 y = x^5 + a_2 x^4 + a_4 x^3 + a_6 x^2 + a_8 x + a_{10} (a_5 \neq 0)$$

can be reduced an equation of the form

$$E : y^2 + a_5 y = x^5 + a_4 x^3 + a_8 x + a_{10} (a_5 \neq 0).$$

Also, suppose that E_1 and E_2 are isomorphic hyperelliptic curves of genus 2 over F_{2^n} given by

$$E_1 : y^2 + a_5 y = x^5 + a_4 x^3 + a_8 x + a_{10} (a_5 \neq 0).$$

$$E_2 : y^2 + \bar{a_5} y = x^5 + \bar{a_4} x^3 + \bar{a_8} x + \bar{a_{10}} (\bar{a_5} \neq 0).$$

Then E_1 is transformed into E_2 by the change of variables (2.3). That is, there exist $\alpha(\neq 0)$, β, γ, δ and ϵ in F_{2^n} such that

$$\begin{cases} \alpha^5 \bar{a_5} = a_5 \\ \alpha^4 \bar{a_4} = a_4 \\ 0 = \gamma^2 + \beta \\ 0 = \gamma a_5 + \beta a_4 + \delta^2 \\ 0 = \alpha^8 \bar{a_8} + a_8 + \delta a_5 + \beta^2 a_4 + \beta^4 \\ 0 = \alpha^{10} \bar{a_{10}} + a_{10} + \beta a_8 + \epsilon a_5 + \beta^3 a_4 + \epsilon^2 + \beta^5. \end{cases}$$

3. A classification of isomorphism classes of hyperelliptic curves of genus 2 over F_{2^n}

Now, we characterize the isomorphism classes of hyperelliptic curves of genus 2 over F_{2^n} for odd n, represented by an equation of the form $y^2 + a_5 y = x^5 + a_8 x + a_{10} (a_5 \neq 0)$. Observe that if $(n, d) = 1$, then $x^{2^d - 1} + a = 0$ has a root in F_{2^n} for any $a \in F_{2^n}$ since $(n, d) = 1$ implies $(2^n - 1, 2^d - 1) = 1$.

Theorem 3.1 Let n be an odd integer. Then a hyperelliptic curve of genus 2 over F_{2^n}, represented by an equation of the form

$$y^2 + a_5 y = x^5 + a_8 x + a_{10} (a_5 \neq 0)$$

is isomorphic to exactly one of following three curves :

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

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

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

Proof Let E' be the curve given by the equation

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

Note that $\{a^5 | a \in F_{2^n}\} = F_{2^n}$ since $(2^n - 1, 5) = 1$. Hence $r = \sqrt[5]{a'_5} \in F_{2^n}$, and so the admissible change of variables

$$(x, y) \to (r^2 x, r^5 y)$$

transforms E' to a curve given by

$$E : y^2 + y = x^5 + a_8 x + a_{10} \tag{3.1}$$

Hence $E' \cong E$ and there are 2^{2n} such curves. If $\bar{E}$ is the curve defined by

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

Then $E \cong \bar{E}$ if and only if there exist $\alpha(\neq 0)$, δ and ϵ in F_{2^n} such that

$$\begin{cases} \alpha^5 = 1 \\ \delta^{16} + \delta + \alpha^3 \bar{a_8} + a_8 = 0 \\ \epsilon^2 + \epsilon + \delta^{20} + a_8 \delta^4 + a_{10} + \bar{a_{10}} = 0. \end{cases}$$

Since $gcd(2^n - 1, 5) = 1$, we get $\alpha = 1$. Hence $E \cong \bar{E}$ if and only if there exist δ and ϵ in F_{2^n} such that

$$\begin{cases} \delta^{16} + \delta + \bar{a_8} + a_8 = 0 \\ \epsilon^2 + \epsilon + \delta^{20} + a_8 \delta^4 + a_{10} + \bar{a_{10}} = 0. \end{cases} \tag{$*$}$$

(1) Suppose that $E_1 \cong \bar{E}$, where E_1 is the curve defined by

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

Then $a_8 = 1$ and $a_{10} = 0$ in $(*)$ imply

$$\delta^{16} + \delta + \bar{a_8} = 0 \tag{3.2}$$

$$\epsilon^2 + \epsilon + \delta^{20} + \bar{a_{10}} = 0. \tag{3.3}$$

Note that $Tr(\bar{a_8}) = Tr(\delta^{16} + \delta) = Tr(\delta^{16}) + Tr(\delta) = 0$. Hence by Proposition 2.2, (3.2) has exactly two roots δ_1 and $\delta_1 + 1$ in F_{2^n}. Note that $Tr((\delta_1 + 1)^{20} + \bar{a_{10}}) = Tr(\delta_1^{20} + 1 + \bar{a_{10}}) = Tr(\delta_1^{20} + \bar{a_{10}}) + 1 \neq Tr(\delta_1^{20} + \bar{a_{10}})$.

Hence (3.2) has exactly one root which is either δ_1 or $\delta_1 + 1$ and in that case (3.2) has two roots with respect to ϵ. Thus a system of (3.2) and (3.3) has two roots. Since there are 2^{2n} admissible changes of variables, there are 2^{2n-1} curves isomorphic to E_1.

(2) Suppose that $E_2 \cong \bar{E}$, where E_2 is the curve defined by

$$E_2 : y^2 + y = x^5 + x.$$

Then $a_8 = 1$and $a_{10} = 0$ in $(*)$ imply

$$\delta^{16} + \delta + \bar{a_8} + 1 = 0 \tag{3.4}$$

$$\epsilon^2 + \epsilon + \delta^{20} + \delta^4 + \bar{a_{10}} = 0. \tag{3.5}$$

Note that $Tr(\bar{a_8}) = Tr(\delta^{16} + \delta + 1) = Tr(\delta^{16}) + Tr(\delta) + Tr(1) = 1$ since $Tr(1) = 1$.

Hence $Tr(\bar{a_8} + 1) = 0$. By Proposition 2.2, (3.4) has exactly two roots δ_2 and $\delta_2 + 1$ in F_{2^n}. Note that $Tr((\delta_2 + 1)^{20} + (\delta_2 + 1)^4 + \bar{a}_{10}) = Tr(\delta_2^{20} + \delta_2^4 + \bar{a_{10}})$. Hence a system of (3.4) and (3.5) has 4 roots in F_{2^n}. Since there are 2^{2n} admissible changes of variables, there are 2^{2n-2} curves isomorphic to E_2.

(3) Suppose that $E_3 \cong \bar{E}$, where E_3 is the curve defined by

$$E_3 : y^2 + y = x^5 + x + 1.$$

Then $a_8 = 1$ and $a_{10} = 1$ in $(*)$ imply

$$\delta^{16} + \delta + \bar{a_8} + 1 = 0 \tag{3.6}$$

$$\epsilon^2 + \epsilon + \delta^{20} + \delta^4 + \bar{a_{10}} + 1 = 0. \tag{3.7}$$

Hence as in (2), $Tr(\bar{a_8} + 1) = 0$. By Proposition 2.2, (3.6) has exactly two roots δ_3 and $\delta_3 + 1$ in F_{2^n}. As in (2), there are 2^{2n-2} curves isomorphic to E_3.

Now, we show no pairs of (1), (2) and (3) are isomorphic.

If $E_1 \cong E_2$, then there exist δ and ϵ in F_{2^n} satisfying both $\delta^{16} + \delta + 1 = 0$ and $\epsilon^2 + \epsilon + \delta^{20} + \delta^4 = 0$. Since $Tr(1) = 1$, $\delta^{16} + \delta + 1 = 0$ has no roots. Hence it is a contradiction. Thus $E_1 \ncong E_2$. If $E_1 \cong E_3$, then there exist δ and ϵ in F_{2^n} satisfying both $\delta^{16} + \delta + 1 = 0$ and $\epsilon^2+\epsilon+\delta^{20}+\delta^4+1 = 0$. Similarly $E_1 \ncong E_3$. If $E_2 \cong E_3$, then there exist δ and ϵ in F_{2^n} satisfying both $\delta^{16}+\delta = 0$ and $\epsilon^2+\epsilon+\delta^{20}+\delta^4+1 = 0$. But a system of $\delta^{16} + \delta = 0$ and $\epsilon^2 + \epsilon + \delta^{20} + \delta^4 + 1 = 0$ has no roots since $Tr(\delta^{20} + \delta^4 + 1) = 0$. Hence $E_2 \ncong E_3$. So, there are 2^{2n} curves isomorphic to either (1), (2) or (3). Also, there are 2^{2n} curves of the form (3.1). Therefore the curve E' must be isomorphic to exactly one among (1), (2) and (3).

References

1. Y. Choie and D. Yun, *Isomorphism classes of hyperelliptic curves of genus 2 over F_q*, preprint.
2. L. H. Encinas, A. J. Menezes and J. M. Masque, *Isomorphism Classes of Genus 2 Hyperelliptic Curves over Finite Fields*, http://www.cacr.math.uwaterloo.ca/ ajmeneze/research.html.
3. N. Koblitz, *Hyperelliptic cryptosystems*, J. cryptology **1** (1989), 139-150.
4. R. Lidl and H. Niederreiter, *Finite fields, Encyclopedia of Math. and its application*, addison-Welsey **20** (1983).
5. A. Menezes, *Applications of Finite Fields*, Kluwer Academic Publishers (1993).
6. A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers (1997).

7. G. Menichetti, *Roots of affine polynomial*, Annals of Discrete Mathematics **30** (1986), 303-310.

*
Chun Soo Choi
Department of Applied Mathematics
Dankook University
Cheonan, Chungnam 330-714, Korea
E-mail: ccsoo@dku.edu

**
Min Surp Rhee
Department of Applied Mathematics
Dankook University
Cheonan, Chungnam 330-714, Korea
E-mail: msrhee@dku.edu