ISOMORPHISM CLASSES OF PICARD CURVES OVER FINITE FIELDS

JONG WON LEE

ABSTRACT. In this paper we determine the number of isomorphism classes of Picard curves, i.e., superelliptic curves $y^3 = f(x)$ of genus three, over finite fields of characteristic different from 3. In the process of doing this we also provide reduced forms of Picard curves together the number of such forms up to isomorphism. In addition to its own theoretical meaning it has applications to cryptography.

1. INTRODUCTION

Starting in around 1985, the theory of elliptic and hyperelliptic curves over finite fields has been of interest for construction of cryptosystems based on the discrete logarithm problem, and elliptic curve cryptography is now at the stage of commercial interest. One of the main reason for interest in these curves is that they provides us a number of finite abelian groups — the so-called Jacobian groups, on which the discrete logarithm problem seems to be far more computationally infeasible than on the multiplicative groups of finite fields.

Recently a new class of curves, which are called superelliptic curves and are generalizations of hyperelliptic curves when the ground field has an odd characteristic, has suggested for constructing public key cryptosystems by Galbraith, Paulus and Smart in [8]. Besides providing an algorithm for the arithmetic on the Jacobian of the superelliptic curves, in the same paper they proved the method of Adleman, DeMarrais and Huang [1] can be extended to the superelliptic curve case. This leads us to restrict our attention to superelliptic curves of small genus. The first such a non-hyperelliptic example is the superelliptic curves of genus three associated to a cubic function field, which has a special name the Picard curve. Like elliptic curve and hyperelliptic curve of genus 2, a Picard curves admits a geometric interpretation of the arithmetic on its Jacobian group which can be exploited for an efficient arithmetic as described in [3]. Furthermore, the fact that the Jacobian group is isomorphic to the ideal class group of the function field can be used to get an explicit formula which makes the arithmetic more efficient [2, 4].

In addition to its own theoretical importance, the computation of isomorphism classes of the above-mentioned curves has a crytographical meaning. Before setting cryptosystem based on the curves it may useful to know how many essentially different choice of curves we may have. Isomorphism classes of elliptic curves [14,

Date: March 30, 2003.

1991 *Mathematics Subject Classification.* Primary:14Q05, 14H45, 11R58, 11H05.

Key words and phrases. Picard curve, superelliptic curve, isomorphism class, algebraic function field.

12, 11] and hyperelliptic curves of genus two over finite fields [7, 5, 6] are now well-understood. In this paper, we determine the number of isomorphism classes of Picard curves over finite fields. In the process of doing this we also provide reduced forms of Picard curves together the number of such forms up to isomorphism.

The remainder of the paper is organized as follows. After giving the basic notions and properties of Picard curves in the next section, we count the number of isomorphism classes of Picard curves over finite fields of characteristic different from 2 and 3 in section 3. Finally, in section 4 we do the same thing for Picard curves over finite fields of even characteristic.

2. The Picard curves

To simplify the exposition, we start with an algebraic function field K over a field k, that is, a finitely generated extension field of k with transcendental degree one in which k is algebraically closed. If $\mathfrak{p}$ is a place (i.e., a discrete valuation ring between k and K) of K, we denote by $v_{\mathfrak{p}}$ the discrete valuation of K corresponding to it. The **degree**, $\deg \mathfrak{p}$, of a place $\mathfrak{p}$ is defined as the extension degree of the residue field of $\mathfrak{p}$ over k. For a divisor $D = \sum n_{\mathfrak{p}}\mathfrak{p}$ (that is, a finite formal sum of places of K) on K, we write $L(D)$ for the k-vector space of elements $f \in K$ with $v_{\mathfrak{p}}(f) + n_{\mathfrak{p}} \geq 0$ for all places $\mathfrak{p}$ of K. Details of algebraic function fields can be found in [13].

The **abstract curve** C_K of K is the (cofinite) topological space consisting of the places of K that is trivial on k together with a sheaf of k-algebras. Two abstract curves C_K and $C_{K'}$ are said to be **isomorphic** (over k) if the algebraic function fields K and K' are isomorphic as k-algebras. For more details concerning with abstract curves, one may consult Hartshorne's book [9]

Definition 2.1. Let k be a field with $\mathrm{char}k \neq 3$. A **Picard curve** over k is the abstract curve of an algebraic function field of the form $k(x, y)$ with relation $y^3 = f(x)$, where $f(X) \in k[X]$ is a separable monic polynomial of degree 4.

In what follows, whenever we refer to "a Picard curve $y^3 = f(x)$ over k", the abstract curve of the algebraic function field $K = k(x, y)$ with relation $y^3 = f(x)$ is always intended.

Remarks 2.2. 1) Let $\mathfrak{p}_\infty$ be a place of K lying over the infinite place of $k(x)$. From the relation $y^3 = f(x)$ it follows that $v_{\mathfrak{p}_\infty}(x) = -3n$ and $v_{\mathfrak{p}_\infty}(y) = -4n$ for some positive integer n. On the other hand, one can show that

$$3n \leq v_{\mathfrak{p}_\infty}(1/x) \cdot \deg(\mathfrak{p}_\infty) \leq [K : k(1/x)] \leq 3$$

and hence we must have $n = 1$. This means that $Y^3 - f(x)$ is the minimal polynomial of y over $k(x)$, that the infinite place of $k(x)$ totally ramifies in K and that the degree of the place $\mathfrak{p}_\infty$ is 1.

2) As a consequence of Riemann-Hurwitz theorem the genus of the Picard curve is given by

$$-2 + \frac{1}{2}\sum_{\mathfrak{p}} (3 - \gcd(3, v_{\mathfrak{p}}(f))) \deg \mathfrak{p},$$

where the $\mathfrak{p}$ runs through the places of $k(x)$; for a proof see [13, III.7.4]. So, the Picard curve has genus 3.

Let $C : y^3 = x^4 + a_3x^3 + a_6x^2 + a_9x + a_{12}$ be a Picard curve over k, and let $\mathfrak{p}_\infty$ denote the unique place of the function field of C lying over the infinite place of $k(x)$. Then $x \in L(3\mathfrak{p}_\infty)$ and $y \in L(4\mathfrak{p}_\infty)$. Since $\deg \mathfrak{p}_\infty = 1$ and since the genus of the Picard curves is 3, by virtue of Riemann-Roch theorem and Clifford's theorem we see that

$$L(3\mathfrak{p}_\infty) = k \oplus kx \quad \text{and} \quad L(4\mathfrak{p}_\infty) = k \oplus kx \oplus ky.$$

Let $\hat{C} : \hat{y}^3 = \hat{x}^4 + \hat{a}_3\hat{x}^3 + \hat{a}_6\hat{x}^2 + \hat{a}_9\hat{x} + \hat{a}_{12}$ be another Picard curve over k which is isomorphic to C. Identifying the function fields of C and $\hat{C}$ as k-algebras yields

$$k \oplus kx = k \oplus k\hat{x} \quad \text{and} \quad k \oplus kx \oplus ky = k \oplus k\hat{x} \oplus k\hat{y}.$$

So, we have $x = \alpha_3\hat{x} + \beta$ and $y = \alpha_4\hat{y} + \gamma\hat{x} + \delta$ for some $\alpha_3, \alpha_4, \beta, \gamma, \delta \in k$ with α_3 and α_4 nonzero. Here, in order to get the equation of $\hat{C}$ by this change of variables we must have $\alpha_3 = \alpha^3$, $\alpha_4 = \alpha^4$ for some nonzero $\alpha \in k$, and $\gamma = \delta = 0$. This proves:

Proposition 2.3. *Let k be a field with* $\mathrm{char}k \neq 3$. *Two Picard curves $C : y^3 = x^4 + a_3x^3 + a_6x^2 + a_9x + a_{12}$ and $\hat{C} : \hat{y}^3 = \hat{x}^4 + \hat{a}_3\hat{x}^3 + \hat{a}_6\hat{x}^2 + \hat{a}_9\hat{x} + \hat{a}_{12}$ over k are isomorphic over k if and only if $x = \alpha^3\hat{x} + \beta$ and $y = \alpha^4\hat{y}$ for some $\alpha \in k^*$ and $\beta \in k$.*

Under the change of variables in the proposition, the coefficients of the Picard curves satisfy the following system of equations:

$$\left\{\begin{array}{rcl} \alpha^3\hat{a}_3 &=& 4\beta + a_3 \\ \alpha^6\hat{a}_6 &=& 6\beta^2 + 3\beta a_3 + a_6 \\ \alpha^9\hat{a}_9 &=& 4\beta^3 + 3\beta^2 a_3 + 2\beta a_6 + a_9 \\ \alpha^{12}\hat{a}_{12} &=& \beta^4 + \beta^3 a_3 + \beta^2 a_6 + \beta a_9 + a_{12} \end{array}\right. \tag{2.1}$$

3. Isomorphism Classes when $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$

In this section we count the isomorphism classes of Picard curves over a finite field $\mathbb{F}_q$ of odd characteristic. The basis idea is as follows. We will consider a collection $\mathcal{P}$ of Picard curves of special form for which any Picard curves is isomorphic to one of elements of $\mathcal{P}$ and the multiplicative group $\mathbb{F}_q^*$ acts on $\mathcal{P}$ such that two curves in $\mathcal{P}$ are isomorphic if and only if they are in the same orbit. We then get the number of isomorphism classes of Picard curves in terms of the number of orbits in $\mathcal{P}$ under the action of $\mathbb{F}_q^*$.

Since $\mathrm{char}\mathbb{F}_q \neq 2$, via change of variables $x = \hat{x} + \frac{a_3}{4}$ and $y = \hat{y}$, each Picard curve $y^3 = x^4 + a_6x^2 + a_9x + a_{12}$ is isomorphic to a Picard curve of the form $y^3 = x^4 + ax^2 + bx + c$. Let $\mathcal{P}$ denote the set of all Picard curves of this form. If two curves in the set $\mathcal{P}$ are isomorphic, then a possible change of variable between them is $x = \alpha^3\hat{x}$ and $y = \alpha^4\hat{y}$ for some nonzero element α in $\mathbb{F}_q$, in which case the system of equations (2.1) becomes

$$\left\{\begin{array}{rcl} \alpha^6\hat{a}_6 &=& a_6 \\ \alpha^9\hat{a}_9 &=& a_9 \\ \alpha^{12}\hat{a}_{12} &=& a_{12} \end{array}\right. \tag{3.1}$$

Hence, the multiplicative group $\mathbb{F}_q^*$ is regarded as to act on $\mathcal{P}$ by

$$\alpha : y^3 = x^4 + ax^2 + bx + c \mapsto y^3 = x^4 + \frac{a}{\alpha^6}x^2 + \frac{b}{\alpha^9}x + \frac{c}{\alpha^{12}}.$$

Note that by definition two Picard curves in $\mathcal{P}$ are isomorphic if and only if they are in an orbit under this action.

So as to determine the number of orbits in $\mathcal{P}$ we first need to know the size of the set $\mathcal{P}$ and the following result tells us that it is $q^3 - q^2$.

Lemma 3.1. *Let $\mathbb{F}_q$ be the finite field of odd characteristic with q elements. Then the number of non-separable polynomials with coefficients in $\mathbb{F}_q$ of the following form is q^2:*

$$x^4 + ax^2 + bx + c. \tag{3.2}$$

Proof. Let N be the set of all non-separable polynomials of the form (3.2). Write N as a disjoint union $N = N_1 \sqcup N_2$, where N_1 consists of the polynomials in N which have a multiple root in $\mathbb{F}_q$. We first determine the cardinality of the set N_2. For this, consider $f(x) \in N_2$ and let α be a multiple root of it. Then, since $f(x)$ is to have all of the conjugates of α over $\mathbb{F}_q$ as its multiple roots, it should be of the form $f(x) = (x^2 - A)^2$, where $A \in \mathbb{F}_q$ and $x^2 - A$ is irreducible over $\mathbb{F}_q$. Clearly, any polynomial of this form belongs to N_2. So, the cardinality of N_2 is equal to the number of quadratic non-residue in $\mathbb{F}_q^*$ and hence $|N_2| = \frac{q-1}{2}$. Now, to determine $|N_1|$ we consider $g(x) = x^4 + ax^2 + bx + c \in N_1$ with a multiple root α in $\mathbb{F}_q$. Then we can write $g(x) = (x-\alpha)^2(x^2 + 2\alpha x + \beta)$ for some $\beta \in \mathbb{F}_q$ with

$$a = -3\alpha^2 + \beta, \quad b = 2\alpha^3 - 2\alpha\beta, \quad c = \alpha^2\beta. \tag{3.3}$$

So, we have a legitimate surjective map $\psi : \mathbb{F}_q \times \mathbb{F}_q \to N_1$ given by $(\alpha, \beta) \mapsto (x-\alpha)^2(x^2+2\alpha x+\beta)$. It follow easily from the equation (3.3) that two pairs (α, β) and (α_1, β_1) are sent to the same non-separable polynomial by ψ if and only if $\alpha^2 = \alpha_1^2 = \beta = \beta_1$. This means that each element in N_1 has at most two preimages, and that the number of elements of N_2 which have two preimages is the same as the number of quadratic non-resides in $\mathbb{F}_q$. Therefore, we have $|N_1| = q^2 - \frac{q-1}{2}$, which proves the lemma. □

Theorem 3.2. *Let $\mathbb{F}_q$ be a finite field of characteristic $\neq 2, 3$ with q elements. Then the number of isomorphism classes of Picard curves over $\mathbb{F}_q$ is*

$$\begin{cases} q^2 + q - 1 & \text{if } q - 1 \equiv 2, 10, 14, 22, 26, 34 \pmod{36}, \\ q^2 + q + 1 & \text{if } q - 1 \equiv 4, 8, 16, 20, 28, 32 \pmod{36}, \\ 3(q^2 + q - 1) & \text{if } q - 1 \equiv 6, 30 \pmod{36}, \\ 3(q^2 + q + 1) & \text{if } q - 1 \equiv 12, 18, 24 \pmod{36}, \\ 3(q^2 + q + 3) & \text{if } q - 1 \equiv 0 \pmod{36}. \end{cases}$$

Proof. We divide the set $\mathcal{P}$ into four disjoint subsets:

$$\begin{aligned} \mathcal{P}_4 &= \left\{ y^3 = x^4 + ax^2 + bx + c \in \mathcal{P} \mid a = b = 0 \neq c \right\}, \\ \mathcal{P}_3 &= \left\{ y^3 = x^4 + ax^2 + bx + c \in \mathcal{P} \mid a = c = 0 \neq b \right\}, \\ \mathcal{P}_2 &= \left\{ y^3 = x^4 + ax^2 + bx + c \in \mathcal{P} \mid b = 0, a \neq 0 \neq c \right\}, \end{aligned}$$

and $\mathcal{P}_1 = \mathcal{P} - \bigcup_{i=2}^4 \mathcal{P}_i$. Clearly, $|\mathcal{P}_4| = |\mathcal{P}_3| = q-1$. Since a polynomial $X^4 + aX^2 + c$ is non-separable if and only if $(\frac{a}{2})^2 = c$, we have $|\mathcal{P}_2| = (q-1)(q-2)$ and hence by the lemma $|\mathcal{P}_1| = q(q-1)^2$. For each i, the set $\mathcal{P}_i$ is stable under the action of $\mathbb{F}_q^*$ on $\mathcal{P}$

and by (3.1) each curve in $\mathcal{P}_i$ has the same isotropy group $G_i = \{\alpha \in \mathbb{F}_q \mid \alpha^{3i} = 1\}$. Hence the number of orbits in $\mathcal{P}$ is

$$\frac{1}{q-1}\sum_{i=1}^{4} |\mathcal{P}_i||G_i| = |G_4| + |G_3| + (q-2)|G_2| + (q^2-q)|G_1|.$$

From the fact that $|G_i| = \gcd(3i, q-1)$, the theorem now follows immediately. □

4. Isomorphism Classes when $\mathrm{char}(\mathbb{F}_q) = 2$

In this final section we count the number of isomorphism classes of Picard curve over a finite of even characteristic. To this end, we first consider three sets of Picard curves such that two curves in different sets cannot be isomorphic and any ismorphism class of Picard curves can be represented by a curve in the union of the sets. We then achieve our goal by counting the isomorphism classes in each set.

Throughout this section, unless specified otherwise, whenever we refer to finite fields, finite fields of characteristic 2 are understood.

Let $\mathbb{F}_q$ be a finite field of characteristic 2. Then any Picard curve over $\mathbb{F}_q$ is isomorphic to one and only one of the following types:

$$y^3 = x^4 + ax^3 + bx + c \text{ with } a \neq 0; \tag{4.1}$$

$$y^3 = x^4 + ax^2 + bx + c \text{ with } a \neq 0 \neq b; \tag{4.2}$$

$$y^3 = x^4 + ax + b \text{ with } a \neq 0. \tag{4.3}$$

Indeed, let a Picard curve $C : y^3 = x^4 + a_3x^3 + a_6^2 + a_9x + a_{12}$ over $\mathbb{F}_q$ be given. First we note that, since $\mathrm{char}\mathbb{F}_q = 2$, the system of equations (2.1) becomes

$$\begin{cases} \alpha^3\hat{a}_3 &= a_3 \\ \alpha^6\hat{a}_6 &= \beta a_3 + a_6 \\ \alpha^9\hat{a}_9 &= \beta^2 a_3 + a_9 \\ \alpha^{12}\hat{a}_{12} &= \beta^4 + \beta^3 a_3 + \beta^2 a_6 + \beta a_9 + a_{12} \end{cases} \tag{4.4}$$

from which we see that any two Picard curves of different types cannot be isomorphic to each other. If a_3 is nonzero, then, taking $\alpha = 1$ and $\beta \in \mathbb{F}_q$ such that $\beta a_3 + a_6 = 0$, we see that the curve is isomorphic to a Picard curve of the form (4.1); in this case we say C is of **type A**. If $a_3 = 0$ and $a_6 \neq 0$, in order for $X^4 + a_3X^3 + a_6X^2 + a_9X + a_{12}$ to be seprable the coefficient a_6 should be nonzero; in this case C is said to be of **type B**. If $a_3 = a_6 = 0$, in order for $X^4 + a_3X^3 + a_6X^2 + a_9X + a_{12}$ to be separable a_9 should be nonzero; in this case C is said to be of **type C**.

We first count isomorphism classes of Picard curves of type A in terms of isomorphism classes of Picard curves of the form (4.1). For this, we need to know the number of such curves.

Lemma 4.1. *The number of separable polynomials over $\mathbb{F}_q$ of the following form is $q(q-1)^2$:*

$$x^4 + ax^3 + bx + c \quad (a \neq 0). \tag{4.5}$$

Proof. We prove this lemma by counting the number of non-separable polynomial of the given form is $q(q-1)$. Let $f(x)$ be a non-separable polynomial of the form (4.5). Then any multiple root, say α, of it should be in $\mathbb{F}_q$. In this case, $f(x)$ can

be written as $f(x) = (x-\alpha)^2(x+\beta x+\alpha^2)$ for some nonzero $\beta \in \mathbb{F}_q$. So, we get a surjective map from $\mathbb{F}_q \times \mathbb{F}_q^*$ to the set of non-separable polynomial of the form (4.5) defined by $(\alpha,\beta) \mapsto (x-\alpha)^2(x+\beta x+\alpha^2)$, which can be easily checked to be injective. This completes the proof. □

Proposition 4.2. *The number of isomorphism classes of Picard curves over $\mathbb{F}_q = \mathbb{F}_{2^m}$ of type A is given by*

$$\begin{cases} q(q-1) & \text{if } m \text{ is odd,} \\ 3q(q-1) & \text{if } m \text{ is even.} \end{cases}$$

Proof. The multiplicative group $\mathbb{F}_q^*$ canonically acts on the set, say Σ of Picard curve of the form (4.1). Each curve in the set Σ has the same isotropy $G = \{\alpha \mid \alpha^3 = 1\}$. So, the number of isomorphism classes in Σ is $\frac{|\Sigma|}{(\mathbb{F}_q^* : G)}$. On the other hand, according to the previous lemma, $|\Sigma| = q(q-1)^2$. Now, the result follows immediately. □

We now count the number of isomorphism classes of Picard curves of type B. Let $\mathcal{B}$ denote the set of Picard curves of the form (4.2). The group $\mathbb{F}_q^* \times \mathbb{F}_q$ acts on $\mathcal{B}$ in the following manner:

$$(\alpha,\beta) : y^3 = x^4 + a_6x^2 + a_9x + a_{12} \mapsto \hat{y}^3 = \hat{x}^4 + \hat{a}_6\hat{x}^2 + \hat{a}_9\hat{x} + \hat{a}_{12},$$

where

$$\begin{cases} \alpha^6\hat{a}_6 &= a_6 \\ \alpha^9\hat{a}_9 &= a_9 \\ \alpha^{12}\hat{a}_{12} &= \beta^4 + \beta^2 a_6 + \beta a_9 + a_{12}. \end{cases} \tag{4.6}$$

The isotropy group of a Picard curve $y^3 = x^4 + a_3x^3 + a_9x + a_{12}$ in $\mathcal{B}$ under this action is the product $G_3 \times G_{a_6,a_9}$, where $G_3 = \{\alpha \in \mathbb{F}_q \mid \alpha^3 = 1\}$ and $G_{a_6,a_9} = \{\beta \in \mathbb{F}_q \mid \beta^4 + a_6\beta^2 + a_9\beta = 0\}$. Note that the separability of the polynomial $X^4 + a_6X^2 + a_9X$ implies $|G_{a_6,a_9}| = 1, 2$ or 4. So, we can write

$$\mathcal{B} = \mathcal{B}_1 \sqcup \mathcal{B}_2 \sqcup \mathcal{B}_4,$$

where each $\mathcal{B}_n$ consists of Picard curves $y^3 = x^4 + a_3x^3 + a_9x + a_{12}$ of type B such that $|G_{a_6,a_9}| = n$.

Lemma 4.3. *Let G_3 and $\mathcal{B}_i$ be as above. Then we have $|\mathcal{B}_2| = \frac{1}{2}q^2(q-1)$ and $|\mathcal{B}_4| = \frac{1}{2}q(q-1)(q-1-|G_3|)$.*

Proof. We first compute $|\mathcal{B}_2|$ by counting the number of cubic polynomials of the form

$$x^3 + ax + b \quad (a, b \in \mathbb{F}_q^*) \tag{4.7}$$

with only one solution in $\mathbb{F}_q$. Let $f(x)$ be such a polynomial and let α denote its unique root lies in $\mathbb{F}_q$. Then we have a following factorization

$$f(x) = (x-\alpha)(x^2 + \alpha x + \beta)$$

for some nonzero $\beta \in \mathbb{F}_q$ such that $x^2 + \alpha x + \beta$ is irreducible. Since $x^2 + \alpha x + \beta$ is irreducible if and only if the absolute trace of $\frac{\beta}{\alpha^2}$ is nonzero and since there are exactly $\frac{q}{2}$ elements of $\mathbb{F}_q$ with nonzero absolute trace, the number of polynomials of the form 4.7 with only one roots in $\mathbb{F}_q$ is $\frac{1}{2}q(q-1)$ and hence $|\mathcal{B}_2| = \frac{1}{2}q^2(q-1)$.

To determine $|\mathcal{B}_4|$, we consider three distinct nonzero elements α, β and γ of $\mathbb{F}_q$. To say that the polynomial $(x-\alpha)(x-\beta)(x-\gamma)$ is of the form (4.7) is equivalent to saying that they satisfy the relations $\alpha+\beta+\gamma=0$ and $\alpha^2+\alpha\beta+\beta^2\neq 0$. So, the cardinality of $\mathcal{B}_4$ is equal to q times the number of ways to find two distinct nonzero elements $\alpha, \beta \in \mathbb{F}_q$ such that $(\frac{\alpha}{\beta})^2+\frac{\alpha}{\beta}+1\neq 0$. Given nonzero $\alpha\in\mathbb{F}_q$, the number of nonzero element $\beta\in\mathbb{F}_q$ different from α such that $(\frac{\alpha}{\beta})^2+\frac{\alpha}{\beta}+1\neq 0$ is $q-1-|G_3|$ and hence the number of cubic polynomials of the form (4.7) is $\frac{1}{2}(q-1)(q-1-|G_3|)$; therefore, we obtain the claimed cardinality of $\mathcal{B}_4$. □

Proposition 4.4. *The number of isomorphism classes of Picard curves over $\mathbb{F}_q=\mathbb{F}_{2^m}$ of type B is given by*

$$\begin{cases} 3q-4 & \text{if } m \text{ is odd,} \\ 9q-21 & \text{if } m \text{ is even.} \end{cases}$$

Proof. According to the rule (4.6) of change of variables and our construction of the sets $\mathcal{B}_i$, it can be checked easily that the sets $\mathcal{B}_i$ are stable under the action of $\mathbb{F}_q^*\times\mathbb{F}_q$ on $\mathcal{B}$. The isotropy group of each element in $\mathcal{B}_i$ has the cardinality $|G_3|\cdot i$. Hence, the number of isomorphism classes of Picard curves of type B is

$$\begin{aligned} &\frac{1}{q(q-1)}\left(|\mathcal{B}_1||G_3|+2|\mathcal{B}_2||G_3|+4|\mathcal{B}_4||G_3|\right) \\ &= \frac{|G_3|}{q(q-1)}\left(|\mathcal{B}|+|\mathcal{B}_2|+3|\mathcal{B}_4|\right) \\ &= |G_3|\left(q-1+\frac{q}{2}+\frac{3}{2}(q-1-|G_3|)\right). \end{aligned}$$

The remaining of the proof now follows easily. □

It now remains to count isomorphism classes of the Picard curves of type C. Let $\mathcal{C}$ be the set of all Picard curves over $\mathbb{F}_q$ of the form (4.3). Proposition 2.3 allows us to regard the group $\mathbb{F}_q^*\times\mathbb{F}_q$ as to act on $\mathcal{C}$ as follows:

$$(\alpha,\beta): y^3=x^4+a_9x+a_{12} \mapsto \hat{y}^3=\hat{x}^4+\hat{a}_9\hat{x}+\hat{a}_{12},$$

where

$$\left\{\begin{array}{rcl} \alpha^9\hat{a}_9 &=& a_9 \\ \alpha^{12}\hat{a}_{12} &=& \beta^4+\beta a_9+a_{12}. \end{array}\right. \tag{4.8}$$

The isopropy group of a Picard curve $y^3=x^4+a_9x+a_{12}$ of type C is

$$G=\left\{(\alpha,\beta)\in\mathbb{F}_q^*\times\mathbb{F}_q \mid \alpha^9=1,\ \beta^4+a_9\beta+a_{12}(\alpha^3-1)=0\right\}.$$

Let $G_9=\left\{\alpha\in\mathbb{F}_q \mid \alpha^9=1\right\}$. We consider three cases depending on the size of G_9.

Case I: $|G_9|=1$**.** The binomial X^3+a_9 is reducible and, since $\mathbb{F}_q$ contains no primitive third root of unity, has only one root in $\mathbb{F}_q$. Hence, $|G|=2$.

Case II: $|G_9|=3$**.** Since $\mathbb{F}_q$ contains a primitive third root of unity we have

$$|G|=\begin{cases} 3 & \text{if } X^3+a_9 \text{ is irreducible over } \mathbb{F}_q, \\ 12 & \text{otherwise.} \end{cases}$$

Case III: $|G_9|=9$**.** If X^3+a_9 is irreducible, then for any $b\in\mathbb{F}_q$ the polynomial X^4+a_9X+b is the product of linear polynomial and an irreducible polynomial

(see [10, Theorem 3.83]) and hence in this case we have $|G| = 9 \cdot 1 = 9$. Now, we suppose that $X^3 + a_9$ is reducible and say $a_9 = A^3$, where $A \in \mathbb{F}_q$. Let α denote a generator of G_9. One can show that $X^4 + X + b$ ($b \in \mathbb{F}_q$) has a root in $\mathbb{F}_q$ if and only if $\mathrm{Tr}(b) = 0$. So, $X^4 + a_9 X + a_{12}(\alpha^{3n} - 1)$ has a root in $\mathbb{F}_q$ if and only if $\mathrm{Tr}\left(\frac{a_{12}(\alpha^{3n}-1)}{A^4}\right) = 0$, in which case all of its four distinct roots are contained in $\mathbb{F}_q$. Note that, since $\alpha^6 + \alpha^3 + 1 = 0$,

$$\mathrm{Tr}\left(\frac{a_{12}\alpha^6}{A^4}\right) + \mathrm{Tr}\left(\frac{a_{12}\alpha^3}{A^4}\right) = \mathrm{Tr}\left(\frac{a_{12}}{A^4}\right)$$

and that, as n runs from 1 to 9, α^{3n} assumes each of $1, \alpha^3, \alpha^6$ exactly three times. If $\mathrm{Tr}\left(\frac{a_{12}}{A^4}\right) = 1$, then either $\mathrm{Tr}\left(\frac{a_{12}\alpha^3}{A^4}\right) = 0$ or $\mathrm{Tr}\left(\frac{a_{12}\alpha^6}{A^4}\right) = 0$ but not both and hence $|G| = 3 \cdot 4 = 12$. If $\mathrm{Tr}\left(\frac{a_{12}}{A^4}\right) = 0$, we have two possibilities

$$\mathrm{Tr}\left(\frac{a_{12}\alpha^6}{A^4}\right) = \mathrm{Tr}\left(\frac{a_{12}\alpha^3}{A^4}\right) = 0$$

or

$$\mathrm{Tr}\left(\frac{a_{12}\alpha^6}{A^4}\right) = \mathrm{Tr}\left(\frac{a_{12}\alpha^3}{A^4}\right) = 1;$$

in the former case $|G| = 9 \cdot 4 = 36$ and in the latter case $|G| = 3 \cdot 4 = 12$.

Proposition 4.5. *The number of isomorphism classes of Picard curves over a finite field $\mathbb{F}_q = \mathbb{F}_{2^m}$ of type C is*

$$\begin{cases} 2 & \text{if } m \text{ is odd}, \\ 6 & \text{if } m \equiv 2, 4 \pmod 6, \\ 12 & \text{if } m \equiv 0 \pmod 6. \end{cases}$$

Proof. When m is odd, since the cardinality of the isotropy group of any curve in $\mathcal{C}$ is 2, that is, since all the orbits in $\mathcal{C}$ have constant length $\frac{1}{2}q(q-1)$, there are two orbits in $\mathcal{C}$.

Suppose that $m \equiv 2, 4 \pmod 6$, equivalently that $|G_9| = 3$. We divide $\mathcal{C}$ into two subsets which are stable under the action on $\mathcal{C}$:

$$\mathcal{C}_{3,1} = \left\{ y^3 = x^4 + ax + b \mid a \notin \mathbb{F}_q^3 \right\},$$
$$\mathcal{C}_{3,2} = \left\{ y^3 = x^4 + ax + b \mid a \in \mathbb{F}_q^3 \right\}.$$

It follows easily that $|\mathcal{C}_{3,1}| = \frac{2}{3}q(q-1)$ and $|\mathcal{C}_{3,2}| = \frac{1}{3}q(q-1)$. Since the cardinality of isotropy groups of the curves in $\mathcal{C}_{3,1}$ (resp. $\mathcal{C}_{3,2}$) is constant, so is the length of orbits and this constant value is given by $\frac{1}{3}q(q-1)$ (resp. $\frac{1}{12}q(q-1)$). Hence the number of isomorphism classes in the sets $\mathcal{C}_{3,1}$ and $\mathcal{C}_{3,2}$ are 2 and 4, respectively.

Now, finally we consider the case when $m \equiv 0 \pmod 6$, equivalently when $|G_9| = 9$. We partition $\mathcal{C}$ into four subsets $\mathcal{C}_{9,i}$ which are stable under the action of $\mathbb{F}_q^* \times \mathbb{F}_q$,

where

$$\mathcal{C}_{9,1} = \left\{ y^3 = x^4 + ax + b \mid a \notin \mathbb{F}_q^3 \right\},$$
$$\mathcal{C}_{9,2} = \left\{ y^3 = x^4 + ax + b \mid a \in \mathbb{F}_q^3, \mathrm{Tr}(ba^{-4/3}) = 1 \right\},$$
$$\mathcal{C}_{9,3} = \left\{ y^3 = x^4 + ax + b \mid a \in \mathbb{F}_q^3, \mathrm{Tr}(b\alpha^3 a^{-4/3}) = \mathrm{Tr}(b\alpha^6 a^{-4/3}) = 0 \right\},$$
$$\mathcal{C}_{9,4} = \left\{ y^3 = x^4 + ax + b \mid a \in \mathbb{F}_q^3, \mathrm{Tr}(b\alpha^3 a^{-4/3}) = \mathrm{Tr}(b\alpha^6 a^{-4/3}) = 1 \right\}.$$

Here, α denotes a generator of G_9. Clearly, $|\mathcal{C}_{9,1}| = \frac{2}{3}q(q-1)$ and $|\mathcal{C}_{9,2}| = \frac{1}{6}q(q-1)$. A simple dimension argument shows that $|\mathcal{C}_{9,3}| = \frac{1}{12}q(q-1)$ and hence we have $|\mathcal{C}_{9,4}| = \frac{1}{12}q(q-1)$. On the other hand, the isotropy groups of curves in $\mathcal{C}_{9,i}$ have the same size as proved and given above. After the very similar argument in the previous paragraph, we see that the number of isomorphism classes in $\mathcal{C}_{9,i}$ are $6, 2, 3, 1$. This completes the proof. □

Finally, combining Propositions 4.2, 4.4 and 4.5, we get the main result of this section.

Theorem 4.6. *The number of isomorphism classes of Picard curves over a finite field $\mathbb{F}_q = \mathbb{F}_{2^m}$ is given by*

$$\begin{cases} q^2 + 2q - 2 & \text{if } m \text{ is odd}, \\ 3(q^2 - 5) & \text{if } m \equiv 2, 4 \pmod 6, \\ 3(q^2 - 3) & \text{if } m \equiv 0 \pmod 6. \end{cases}$$

References

[1] L.M. Adleman, J. DeMarrais and M.D. Huang. *A subexpoential algorithm for discrete logarithms over hyperelliptic curves of large genus over GF(q)*, Theoretical Computer Science **226** (1999), 7–18.

[2] M. L. Bauer. *The arithmetic of certain cubic function fields*, preprint, 2002.

[3] E.R. Barreiro, J.P. Cherdieu, and J.E. Sarlabous. *Efficient reduction on the Jacobian variety of Picard curves*, Coding theory, cryptology and related areas, Springer-Verlag, 2000.

[4] A. Basiri, A. Enge, J.P. Faugère, and N. Gürel. *The arithmetic of Jacobian groups of superelliptic curves*, preprint, 2002.

[5] Y. Choie and D. Yun. *Isomorphism classes of hyperelliptic curves of genus 2 over $\mathbb{F}_q$*, preprint, 2001.

[6] L.H. Encinas and J.M. Masqué. *Isomorphism Classes of Hyperelliptic Curves of Genus 2 in Characteristic 5*, preprint.

[7] L.H. Encinas, A. Menezes, and J.M. Masqué. *Isomorphism Classes of Genus-2 Hyperelliptic Curves over Finite Fields*, preprint.

[8] S. D. Galbraith, S. M. Paulus, and N. P. Smart. *Arithmetic on Superelliptic Curves*, Math. Comp., **71** (2000), no. 237, 393–405.

[9] R. Hartshorne. *Algebraic Geometry*, GTM **52**, Springer-Verlag, 1977.

[10] R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications*, Cambridge University Press, 1994.

[11] A. Menezes and S. Vanstone. *Isomorphism classes of elliptic curves over finite field of characterisitc 2*, Utilitas Mathematica, **38** (1990), 135–154.

[12] R. Schoof. *Nonsingular plane cubic curves over finite fields*, Journal of Combinatorial Theory, **46** (1987), 183–211.

[13] H. Stichtenoth. *Algebraic Function Fields and Codes*, Universitext, Springer-Verlag, 1993.

[14] E. Waterhouse. *Abelian Varieties over finite fields*, Ann. Sci. École Norm. Sup., **2** (1969), 521–560.

Institut für Experimentelle Mathematik, Universität Essen, Ellernstrasse 29, 45326 Essen, Germany

E-mail address: lee@exp-math.uni-essen.de

URL: http://www.exp-math.uni-essen.de/~lee