Isomorphism classes of hyperelliptic curves of genus 3 over finite fields

Yingpu Deng

Institute of Systems Science, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China

Received 2 February 2004; revised 3 May 2005

Communicated by Neal Koblitz

Available online 28 June 2005

Abstract

In this paper we present a direct method to compute the number of isomorphism classes of hyperelliptic curves of genus 3 over finite fields \( \mathbb{F}_q \). The number of isomorphism classes is a polynomial in \( q \) of degree 5. In all the cases we show an explicit formula for this polynomial. These results can be used in the classification problems and the hyperelliptic curve cryptosystems.

© 2005 Elsevier Inc. All rights reserved.

MSC: primary 11G20; secondary 94A60

Keywords: Hyperelliptic curves; Hyperelliptic curve cryptosystems; Jacobians; Isomorphism classes; Stabilizer

1. Introduction

In 1989, Koblitz [12] proposed that the Jacobians of hyperelliptic curves of genus \( g \) over finite fields (if \( g = 1 \), then it is the additive groups of elliptic curves) can be applied to construct the public key cryptosystems, that is hyperelliptic curve cryptosystems (HECC). In fact, we only need to use all the constructions of elliptic curve
cryptosystems (ECC), but with the additive groups of elliptic curves replaced by the Jacobians \( J(\mathbb{F}_q) \) of hyperelliptic curves. The basic operation required to implement the system is the computation of \( kD \) for a large integer \( k \) and an element \( D \) of \( J(\mathbb{F}_q) \). Cantor’s algorithms [2] showed an efficient implementation for such an operation. Since the security of such cryptosystem relies upon the presumed difficulty of solving discrete logarithm problem in the Jacobians \( J(\mathbb{F}_q) \), that is hyperelliptic curve discrete logarithm problem (HECDLP), many people pay attention to study the hyperelliptic curve discrete logarithm problem. On the other hand, since there are surprising results, that is, if the genus \( g \) of a hyperelliptic curve is large enough, then there is a subexponential algorithm for HECDLP over finite fields (see [1,9]), and if the genus \( g > 4 \), then there exists an algorithm solving HECDLP over finite fields that is better than the Pollard’s rho algorithm (see [10]), hence people focus their attention on the cases \( g = 2, 3, 4 \), especially \( g = 2, 3 \). Since the order of a Jacobian of a hyperelliptic curve of genus \( g \) over the finite field \( \mathbb{F}_q \) approximately equals to \( q^g \) by the Weil theorem, for \( g = 2 \), if take \( q \approx 2^{80} \), then \( q^g \approx 2^{160} \). It implies that the security of genus-2 HECC with a secret key of length 80 bits is of the same level as that of ECC with a secret key of length 160 bits, and that of the multiplicative group cryptosystems over finite fields with a secret key of length 1024 bits. For \( g = 3 \), if take \( q \approx 2^{54} \), then \( q^g \approx 2^{160} \). It implies that the security of genus-3 HECC with a secret key of length 54 bits is of the same level as that of ECC with a secret key of length 160 bits. Therefore, from cryptographic point of view, HECC is of the superiority of short secret keys and strong security, hence people are interested in studying for the cases \( g = 2, 3, 4 \). In order to study HECC, first we need to answer how many hyperelliptic curves over finite fields can be applied to the cryptosystems. Since the Jacobians of two isomorphic hyperelliptic curves are isomorphic as abelian groups, two isomorphic hyperelliptic curves are the same from the cryptographic point of view. The problem turns into counting the number of isomorphism classes of hyperelliptic curves. Encinas et al. [8] showed a formula of the number of isomorphism classes of hyperelliptic curves of genus 2 over the finite field \( \mathbb{F}_q \) while the characteristic of the fields \( \text{char}(\mathbb{F}_q) \neq 2, 5 \). Later Encinas and Masqué [7] gave a similar formula while \( \text{char}(\mathbb{F}_q) = 5 \). For \( \text{char}(\mathbb{F}_q) = 2 \), Choie and Yun [5] gave some upper and lower bounds for the number of isomorphism classes of hyperelliptic curves of genus 2, and Deng and Liu [6] completely determined the number of isomorphism classes of hyperelliptic curves of genus 2 over finite fields with even characteristic. For \( g = 3 \), when \( \text{char}(\mathbb{F}_q) \neq 2, 7 \), Jeong [11] gave the exact formulae for the number of isomorphism classes, but his results are incomplete; When \( \text{char}(\mathbb{F}_q) = 7 \), Choie and Jeong [4] obtained some bounds for the number. Note that in this paper, we consider hyperelliptic curves with a Weierstrass point. For the general hyperelliptic curves, the number of curves is obtained in [16].

In this paper we present a direct method to compute the number of isomorphism classes of hyperelliptic curves of genus 3 over finite fields \( \mathbb{F}_q \), the number of isomorphism classes is the polynomials in \( q \) of degree 5. In all the cases we show an explicit formula for this polynomial. This paper is organized as follows. We give some preliminaries in Section 2. In Section 3 we give some results for counting the separable polynomials over finite fields. In Section 4 we consider the case \( \text{char}(\mathbb{F}_q) \neq 2, 7 \), we will give the complete answers. In Section 5 we consider the case \( \text{char}(\mathbb{F}_q) = 7 \), we will
give the exact value for the number of isomorphism classes. In Section 6 we consider the case \( \text{char}(\mathbb{F}_q) = 2 \), we also give the exact value for the number of isomorphism classes.

2. Preliminaries

A good elementary introduction to hyperelliptic curves can be found in [15].

Let \( \mathbb{F}_q \) be the finite field of \( q \) elements, and let \( \overline{\mathbb{F}}_q \) be the algebraic closure of \( \mathbb{F}_q \). A hyperelliptic curve \( C \) of genus \( g (g \geq 1) \) over \( \mathbb{F}_q \) is a projective non-singular irreducible curve of genus \( g \) defined over \( \mathbb{F}_q \) for which there exists a map \( C \rightarrow \mathbb{P}^1(\overline{\mathbb{F}}_q) \) of degree two, where \( \mathbb{P}^1(\overline{\mathbb{F}}_q) \) denotes the 1-dimensional projective space over \( \overline{\mathbb{F}}_q \). As in [14], we further assume that \( C \) has an \( \mathbb{F}_q \)-rational point \( P \) such that the \( \mathbb{F}_q \)-rational function field of \( C \) has a nonconstant function whose only pole is a double one at \( P \). Such a point is called a Weierstrass point. Let \( \mathcal{I}_g \) denote the set of all hyperelliptic curves of genus \( g \) over \( \mathbb{F}_q \).

Two curves in \( \mathcal{I}_g \) are said to be isomorphic over \( \mathbb{F}_q \) if they are isomorphic as projective varieties over \( \mathbb{F}_q \). The isomorphic relation over \( \mathbb{F}_q \) is an equivalence relation on \( \mathcal{I}_g \). If two curves \( C_1, C_2 \) in \( \mathcal{I}_g \) are isomorphic over \( \mathbb{F}_q \), then their Jacobians \( \mathcal{J}_{C_1}(\mathbb{F}_q), \mathcal{J}_{C_2}(\mathbb{F}_q) \) are isomorphic as abelian groups. But the reverse is not true.

A Weierstrass equation \( H \) of genus \( g \) over \( \mathbb{F}_q \) is an equation of the form

\[
H : \quad v^2 + h(u)v = f(u) \quad \text{in} \quad \mathbb{F}_q[u,v],
\]

where \( h(u) \in \mathbb{F}_q[u] \) is a polynomial of degree at most \( g \), i.e., \( \deg(h(u)) \leq g \), and \( f(u) \in \mathbb{F}_q[u] \) is a monic polynomial of degree \( 2g + 1 \), i.e., \( \deg(f(u)) = 2g + 1 \), and there are no singular affine points, i.e., there are no \((x, y) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q\) satisfying

\[
\begin{align*}
\frac{y^2 + h(x)y}{2} &= f(x), \\
2y + h(x) &= 0, \\
h'(x)y - f'(x) &= 0.
\end{align*}
\]

For \( \text{char}(\mathbb{F}_q) \neq 2 \), this is equivalent to say that the polynomial \( f(u) + \frac{1}{4}h^2(u) \) has no multiple roots. Let \( \mathfrak{M}_g \) denote the set of all Weierstrass equations of genus \( g \).

**Proposition 2.1** (Lockhart [14]). There is a 1–1 correspondence between isomorphism classes of curves in \( \mathcal{I}_g \) and equivalence classes of Weierstrass equations in \( \mathfrak{M}_g \), where \( H_1, H_2 \in \mathfrak{M}_g \) are said to be equivalent over \( \mathbb{F}_q \) if there exist \( \alpha, \beta \in \mathbb{F}_q \) with \( \alpha \neq 0 \), and \( t \in \mathbb{F}_q[u] \) with \( \deg(t) \leq g \), such that the coordinate transformation

\[
(u, v) \mapsto (\alpha^2u + \beta, \alpha^{2g+1}v + t)
\]

transforms equation \( H_1 \) to equation \( H_2 \).
Thus to count the number of isomorphism classes in $\mathfrak{I}_g$, it is enough to count the number of equivalence classes of Weierstrass equations in $\mathfrak{M}_g$. This is the number of orbits in $\mathfrak{M}_g$ under the action of the group of the coordinate transformation in Proposition 2.1. The magnitude level of this number is $q^{2g-1}$. For $g = 1$, Schoof [17] verified this consequence. For $g = 2$, Encinas et al. [8], Encinas and Masqué [7], Deng and Liu [6] also verified it. In the rest of the paper, the coordinate transformation refers that in Proposition 2.1.

**Theorem 2.2** (Schoof [17]). The number of isomorphism classes of elliptic curves over the finite field $\mathbb{F}_q$ is

$$2q + 3 + \left(\frac{-3}{q}\right) + 2 \left(\frac{-4}{q}\right),$$

where $\left(\frac{u}{q}\right)$ is Jacobi symbol for $q$ odd and $\left(\frac{n}{2}\right) = (-1)^{n^2-1} / 8$ for $n$ odd and $\left(\frac{n}{2}\right) = 0$ for $n$ even.

For the convenience of the reader, we recall some basic concepts about acting on sets of groups. Let $G$ be a finite group, $X$ be a finite nonempty set. An action of $G$ on the set $X$ is a map

$$G \times X \rightarrow X, \quad (g, x) \mapsto g x,$$

where $g \in G$, $x \in X$, $g x \in X$,

satisfying

$$(gh)x = g(hx), \quad 1x = x, \quad \forall g, h \in G, \quad x \in X,$$

where 1 is the identity of $G$. For $x \in X$, the stabilizer $G_x$ at $x$ is a subgroup of $G$ defined by

$$G_x = \{ g \in G \mid gx = x \}. $$

The length of the orbit $Gx = \{ gx \mid g \in G \}$ containing $x$ is determined by the formula

$$|Gx| = \frac{|G|}{|G_x|}.$$

For $g = 3$, putting

$$h(u) = a_1 u^3 + a_3 u^2 + a_5 u + a_7,$$

$$f(u) = u^7 + a_2 u^6 + a_4 u^5 + a_6 u^4 + a_8 u^3 + a_{10} u^2 + a_{12} u + a_{14},$$

$$t = x^6 u^3 + x^4 \delta u^2 + x^2 \delta u + \epsilon,$$

by Proposition 2.1, under the coordinate transformation

$$(u, v) \mapsto (x^2 u + \beta, x^7 v + t),$$
the formula between the coefficients \( a_i, \bar{a}_i \) \((i = 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14)\) of two Weierstrass equations is

\[
\begin{align*}
\varepsilon a_1 & = 2\gamma + a_1, \\
x^3 a_3 & = 2\delta + 3\beta a_1 + a_3, \\
x^5 a_5 & = 2\theta + 3\beta^2 a_1 + 2\beta a_3 + a_5, \\
x^7 a_7 & = 2\varepsilon + \beta^3 a_1 + \beta^2 a_3 + \beta a_5 + a_7, \\
x^2 a_2 & = 7\beta - \gamma^2 - \gamma a_1 + a_2, \\
x^4 a_4 & = 21\beta^2 - 2\gamma \delta - (\delta + 3\beta \gamma) a_1 + 6\beta a_2 - \gamma a_3 + a_4, \\
x^6 a_6 & = 35\beta^3 - \delta^2 - 2\gamma \theta - (\theta + 3\beta \delta + 3\beta^2 \gamma) a_1 \\
& \quad + 15\beta^2 a_2 - (\delta + 2\beta \gamma) a_3 + 5\beta a_4 - \gamma a_5 + a_6, \\
x^8 a_8 & = 35\beta^4 - 2\gamma \varepsilon - 2\delta \theta - (\varepsilon + 3\beta \theta + 3\beta^2 \delta + \beta^3 \gamma) a_1 + 20\beta^3 a_2 \\
& \quad - (\theta + 2\beta \delta + \beta^2 \gamma) a_3 + 10\beta^2 a_4 \\
& \quad - (\delta + \beta \gamma) a_5 + 4\beta a_6 - \gamma a_7 + a_8, \\
x^{10} a_{10} & = 21\beta^5 - \theta^2 - 2\delta \varepsilon - (3\beta \varepsilon + 3\beta^2 \theta + \beta^3 \delta) a_1 \\
& \quad + 15\beta^4 a_2 - (\varepsilon + 2\beta \theta + \beta^2 \delta) a_3 \\
& \quad + 10\beta^3 a_4 - (\theta + \beta \delta) a_5 + 6\beta^2 a_6 - \delta a_7 + 3\beta a_8 + a_{10}, \\
x^{12} a_{12} & = 7\beta^6 - 20\varepsilon - (3\beta^2 \varepsilon + \beta^3 \theta) a_1 \\
& \quad + 6\beta^5 a_2 - (2\beta \varepsilon + \beta^2 \theta) a_3 + 5\beta^4 a_4 \\
& \quad - (\varepsilon + \beta \theta) a_5 + 4\beta^3 a_6 - \theta a_7 + 3\beta^2 a_8 + 2\beta a_{10} + a_{12}, \\
x^{14} a_{14} & = \beta^7 - \varepsilon^2 - \beta^3 \varepsilon a_1 + \beta^6 a_2 - \beta^2 \varepsilon a_3 + \beta^5 a_4 - \beta \varepsilon a_5 + \beta^4 a_6 \\
& \quad - \varepsilon a_7 + \beta^3 a_8 + \beta^2 a_{10} + \beta a_{12} + a_{14}.
\end{align*}
\]

We will use this formula to transform the Weierstrass equations of hyperelliptic curves into the reduced forms. Under the coordinate transformation in Proposition 2.1 we will analyze the order of the group of the coordinate transformation and the size of the stabilizer to compute the number of orbits of Weierstrass equations under the action of the group of the coordinate transformation. However we must first count the number of Weierstrass equations of various reduced forms. In the next section we concentrate some general results about it to be used in the forthcoming sections.

3. Counting the separable polynomials over finite fields

If a polynomial has no multiple roots, then it is called separable. In this section, we will give some results for counting the separable polynomials over the finite field \( \mathbb{F}_q \) to be used in the forthcoming sections.

Let \( F \) be a field, \( f(X) \) be a monic polynomial of degree \( n(>1) \) over \( F \). The discriminant of \( f \) is defined by

\[
\text{Disc}(f) = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2,
\]
where $x_1, \ldots, x_n$ are all the roots of $f$ in the algebraic closure $\overline{F}$ of $F$. $\text{Disc}(f)$ is an element of $F$. Obviously, $f$ is separable if and only if $\text{Disc}(f) \neq 0$. We will use the notation $\text{Res}(f, g)$ to refer the resultant of two polynomials $f$ and $g$. It is well known that we have $\text{Disc}(f) = (-1)^{\frac{n(n-1)}{2}} \text{Res}(f, f') = \pm \text{Res}(f, f')$, where $f'$ is the derivative of $f$. Hence we have that $f$ is separable if and only if $\text{Res}(f, f') \neq 0$.

For $n \geq 2$, define $N_n = \# \{ f(X) = X^n + a_1 X^{n-1} + a_2 X^{n-2} + \cdots + a_{n-1} X + a_n \in \mathbb{F}_q[X] \mid f \text{ is separable} \}$. The value of $N_n$ is obtained by Carlitz [3].

**Theorem 3.1 (Carlitz [3]).** Using the above notations, we have $N_n = q^n - q^{n-1}$ for $n > 1$.

Now we give another method to compute the value of $N_n$. Since finite fields are perfect, so any irreducible polynomial over finite fields is separable, and the product of distinct irreducible polynomials is separable. Let $I_d$ denote the number of monic irreducible polynomials over $\mathbb{F}_q$ of degree $d (> 0)$, it is well known that we have the following.

**Lemma 3.2 (Lidl and Niederreiter [13]).**

$$I_d = \frac{1}{d} \sum_{i|d} \mu(i) q^{d/i},$$

where $\mu$ is the Möbius function.

For a monic separable polynomial over $\mathbb{F}_q$ of degree $n$, consider its decomposition over $\mathbb{F}_q$ into the product of irreducible factors, we know that each decomposition of the polynomial corresponds a partition of $n$. Concretely, suppose

$$\pi = (i_1^{a_1}, \ldots, i_d^{a_d})$$

is a partition of $n$, where $d > 0, i_1 > i_2 > \cdots > i_d > 0, a_1 > 0, \ldots, a_d > 0$, and $n = a_1 i_1 + \cdots + a_d i_d$. Denote by $I_\pi$ the number of monic separable polynomials over $\mathbb{F}_q$ of degree $n$ which decompose as the product over $\mathbb{F}_q$ of $a_1$ many monic irreducible polynomials of degree $i_1, a_2$ many monic irreducible polynomials of degree $i_2, \ldots$, and $a_d$ many monic irreducible polynomials of degree $i_d$, then we have

$$I_\pi = \prod_{j=1}^{d} \binom{I_{i_j}}{a_j}.$$

Hence we have

$$N_n = \sum_\pi I_\pi,$$

where the summation is over all the partitions of $n$. 
**Proposition 3.3.** Using the above notations, we have

\[ N_n = \sum_{\pi} \prod_{j=1}^{d} \left( \frac{I_{ij}}{a_j} \right), \]

where the summation is over all the partitions of \( n \).

In fact, we can give another proof for Theorem 3.1 by using Proposition 3.3. Here we omit the proof.

Sometimes we also need to count the number of monic separable polynomials of degree \( n \) without the second term. For \( n \geq 2 \), define \( M_n = \# \{ f(X) = X^n + a_1 X^{n-1} + a_2 X^{n-2} + \cdots + a_{n-1} X + a_n \in \mathbb{F}_q[X] \mid a_1 = 0, f \text{ is separable} \} \).

**Proposition 3.4.** If \( \gcd(n, q) = 1 \), then we have \( M_n = q^{n-1} - q^{n-2} \).

**Proof.** Putting \( A = \{ f(X) = X^n + a_1 X^{n-1} + a_2 X^{n-2} + \cdots + a_{n-1} X + a_n \in \mathbb{F}_q[X] \mid f \text{ is separable} \}, B = \{ f(X) = X^n + a_1 X^{n-1} + a_2 X^{n-2} + \cdots + a_{n-1} X + a_n \in \mathbb{F}_q[X] \mid a_1 = 0, f \text{ is separable} \}. \) For \( f \in A \), since \( \gcd(n, q) = 1 \), it is easy to see \( f(X - \frac{a_1}{n}) \in B \). Thus we have a mapping \( \sigma : A \to B, \sigma(f(X)) = f(X - \frac{a_1}{n}) \). Obviously, \( \sigma \) is surjective, and it maps each \( q \) polynomials in \( A \) into one polynomial in \( B \). Therefore we have \( |B| = \frac{|A|}{q} \). This completes the proof. \( \square \)

The condition \( \gcd(n, q) = 1 \) in Proposition 3.4 is necessary. For example, when \( n = 2, \text{char}(\mathbb{F}_q) = 2, f(X) = X^2 + a_2 \). Obviously \( f \) is always not separable, hence we have \( M_n = 0 \neq q - 1 \).

We also need a result in the forthcoming sections.

**Proposition 3.5.** Define

\[ L_1 = \# \{ f(X) = X^3 + a_1 X^2 + a_2 X + a_3 \in \mathbb{F}_q[X] \mid f \text{ is separable and } a_1 = a_2 = 0, a_3 \neq 0 \}, \]

\[ L_2 = \# \{ f(X) = X^3 + a_1 X^2 + a_2 X + a_3 \in \mathbb{F}_q[X] \mid f \text{ is separable and } a_1 = a_3 = 0, a_2 \neq 0 \}, \]

\[ L_3 = \# \{ f(X) = X^3 + a_1 X^2 + a_2 X + a_3 \in \mathbb{F}_q[X] \mid f \text{ is separable and } a_1 = 0, a_2 \neq 0, a_3 \neq 0 \}. \]
\[ L_4 = \sharp \{ f(X) = X^3 + a_1X^2 + a_2X + a_3 \in \mathbb{F}_q[X] \mid f \text{ is separable and } a_2 = 0, a_1 \neq 0, a_3 \neq 0 \}, \]

\[ L_5 = \sharp \{ f(X) = X^3 + a_1X^2 + a_2X + a_3 \in \mathbb{F}_q[X] \mid f \text{ is separable and } a_3 = 0, a_1 \neq 0, a_2 \neq 0 \}, \]

\[ L_6 = \sharp \{ f(X) = X^3 + a_1X^2 + a_2X + a_3 \in \mathbb{F}_q[X] \mid f \text{ is separable and } a_1 \neq 0, a_2 \neq 0, a_3 \neq 0 \}, \]

then we have

<table>
<thead>
<tr>
<th>char(\mathbb{F}_q) = 2</th>
<th>char(\mathbb{F}_q) = 3</th>
<th>char(\mathbb{F}_q) \neq 2, 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>( L_1 )</td>
<td>( q - 1 )</td>
<td>( q - 1 )</td>
</tr>
<tr>
<td>( L_2 )</td>
<td>( 0 )</td>
<td>( q - 1 )</td>
</tr>
<tr>
<td>( L_3 )</td>
<td>( (q - 1)^2 )</td>
<td>( (q - 1)^2 )</td>
</tr>
<tr>
<td>( L_4 )</td>
<td>( (q - 1)^2 )</td>
<td>( (q - 1)(q - 2) )</td>
</tr>
<tr>
<td>( L_5 )</td>
<td>( (q - 1)^2 )</td>
<td>( (q - 1)(q - 2) )</td>
</tr>
<tr>
<td>( L_6 )</td>
<td>( (q - 1)^2(q - 2) )</td>
<td>( (q - 1)(q^2 - 3q + 3) )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>( (q - 1)(q^2 - 3q + 4) )</td>
</tr>
</tbody>
</table>

**Proof.** Suppose \( f(X) = X^3 + a_1X^2 + a_2X + a_3 \in \mathbb{F}_q[X] \) is separable. By Theorem 3.1, we know that the total number of \( f \) is \( q^3 - q^2 \). Since \( a_2, a_3 \) are not all zeros, so there are only six cases listed in Proposition 3.5. Now we will analyze each case. For \( a_1 = a_2 = 0, a_3 \neq 0 \), \( f(X) = X^3 + a_3 \), \( \text{Res}(f, f') = 27a_3^2 \). When char(\mathbb{F}_q) = 3, the number of this kind of \( f \) is 0; When char(\mathbb{F}_q) \neq 3, the number of this kind of \( f \) is \( q - 1 \). For \( a_1 = a_3 = 0, a_2 \neq 0 \), \( f(X) = X^3 + a_2X = X(X^2 + a_2) \). When char(\mathbb{F}_q) = 2, the number of this kind of \( f \) is 0; When char(\mathbb{F}_q) \neq 2, the number of this kind of \( f \) is \( q - 1 \). For \( a_1 = 0, a_2 \neq 0, a_3 \neq 0 \), \( f(X) = X^3 + a_2X + a_3 \), \( \text{Res}(f, f') = 4a_2^3 + 27a_3^2 \). When char(\mathbb{F}_q) = 2, the number of this kind of \( f \) is \( (q - 1)^2 \). When char(\mathbb{F}_q) \neq 2, 3, since \( 4a_2^3 + 27a_3^2 = 0 \), i.e. \( (\frac{a_2}{3})^3 = (\frac{a_3}{3})^2 \), hence the number of this kind of \( f \) is \( (q - 1)^2 - \frac{a_2^3}{27} \cdot 2 = (q - 1)(q - 2) \). For \( a_2 = 0, a_1 \neq 0, a_3 \neq 0 \), \( f(X) = X^3 + a_1X^2 + a_3 \), \( \text{Res}(f, f') = a_3(4a_1^3 + 27a_3) \). When char(\mathbb{F}_q) = 2, the number of this kind of \( f \) is \( (q - 1)^2 \). When char(\mathbb{F}_q) = 3, the number of this kind of \( f \) is \( (q - 1)^2 \). When char(\mathbb{F}_q) \neq 2, 3, the number of this kind of \( f \) is \( (q - 1)(q - 2) \). For \( a_3 = 0, a_1 \neq 0, a_2 \neq 0 \), \( f(X) = X^3 + a_1X^2 + a_2X = X(X^2 + a_1X + a_2) = Xf_1(X), f_1(X) = X^2 + a_1X + a_2 \), \( \text{Res}(f_1, f_1') = 4a_2 - a_1^2 \). When char(\mathbb{F}_q) = 2, the number of this kind of \( f \) is \( (q - 1)^2 \). When char(\mathbb{F}_q) \neq 2, the number of this kind of \( f \) is \( (q - 1)(q - 2) \). Thus we have computed the values of \( L_1, L_2, L_3, L_4 \) and \( L_5 \), and \( L_6 = q^3 - q^2 - L_1 - L_2 - L_3 - L_4 - L_5 \). This completes the proof. □
4. \text{Char}(\mathbb{F}_q) \neq 2, 7

In this section we suppose \text{char}(\mathbb{F}_q) \neq 2, 7. Putting

\[ \gamma = -\frac{a_1}{2}, \]
\[ \beta = \frac{1}{2}(\gamma^2 + \gamma a_1 - a_2) = -\frac{1}{28}a_1^2 - \frac{1}{4}a_2, \]
\[ \delta = -\frac{1}{2}(3\beta a_1 + a_3) = \frac{3}{56}a_1^3 + \frac{3}{14}a_1 a_2 - \frac{1}{2}a_3, \]
\[ \theta = -\frac{1}{2}(3\beta^2 a_1 + 2\beta a_3 + a_5) = -\frac{3}{1568}a_1^5 - \frac{3}{196}a_1^3 a_2 - \frac{3}{98}a_1 a_2^2 + \frac{2}{28}a_1^2 a_3 + \frac{1}{7}a_2 a_3 - \frac{1}{2}a_5, \]
\[ \varepsilon = -\frac{1}{2}(\beta^3 a_1 + \beta^2 a_3 + \beta a_5 + a_7) \]
\[ = \frac{1}{43904}a_1^7 + \frac{3}{10976}a_1^5 a_2 + \frac{3}{2744}a_1^3 a_2^2 + \frac{1}{686}a_1 a_2^3 \]
\[ - \frac{1}{1568}a_1^4 a_3 - \frac{1}{196}a_1^2 a_2 a_3 - \frac{1}{98}a_2^3 a_3 + \frac{1}{56}a_1^2 a_5 + \frac{1}{14}a_2 a_5 - \frac{1}{2}a_7, \]

in (1), we have \( \bar{a}_1 = \bar{a}_3 = \bar{a}_5 = \bar{a}_7 = \bar{a}_2 = 0. \) That is, we can transform the Weierstrass equation into

\[ v^2 = u^7 + a_4 u^5 + a_6 u^4 + a_8 u^3 + a_{10} u^2 + a_{12} u + a_{14}. \]

Define \( f(u) = u^7 + a_4 u^5 + a_6 u^4 + a_8 u^3 + a_{10} u^2 + a_{12} u + a_{14}. \) Eq. (2) represents a hyperelliptic curve if and only if \( f \) is separable. By Proposition 3.4, the total number of \( f \) is \( q^6 - q^5. \) The coordinate transformation between two Weierstrass equations of form (2), since \( a_i = \bar{a}_i = 0(i = 1, 2, 3, 5, 7), \) as (1), we have necessarily \( \beta = \gamma = \delta = \theta = \varepsilon = 0. \) The coordinate transformation is

\[ (u, v) \mapsto (x^2 u, x^7 v), \quad x \in \mathbb{F}_q^*, \]

and the order of the group of the coordinate transformation is \( q - 1. \)

The formula between the coefficients of two Weierstrass equations is

\[ \begin{aligned}
    x^4 \bar{a}_4 &= a_4, \\
    x^6 \bar{a}_6 &= a_6, \\
    x^8 \bar{a}_8 &= a_8, \\
    x^{10} \bar{a}_{10} &= a_{10}, \\
    x^{12} \bar{a}_{12} &= a_{12}, \\
    x^{14} \bar{a}_{14} &= a_{14}.
\end{aligned} \]

Define \( \mathcal{H} = \{ f(u) = u^7 + a_4 u^5 + a_6 u^4 + a_8 u^3 + a_{10} u^2 + a_{12} u + a_{14} \in \mathbb{F}_q[u] \mid f \text{ is separable} \}, |\mathcal{H}| = q^6 - q^5. \) The group of the coordinate transformation is denoted by \( G, \ G \cong \mathbb{F}_q^*, |G| = q - 1. \) For \( f \in \mathcal{H}, \) the stabilizer at \( f \) is denoted by \( G_f. \) If \( f \in \mathcal{H}, \) the stabilizer at \( f \) is denoted by \( G_f. \) We know that the length of the orbit containing \( f \) is \( (G : G_f). \) We will analyze the size
of the stabilizer $G_f$. By (3), in the stabilizer $G_f$ at $f$ we have

$$
\begin{cases}
x^4a_4 = a_4, \\
x^6a_6 = a_6, \\
x^8a_8 = a_8, \\
x^{10}a_{10} = a_{10}, \\
x^{12}a_{12} = a_{12}, \\
x^{14}a_{14} = a_{14}.
\end{cases}
$$

(4)

Define $\mathcal{H}_1 = \{ f \in \mathcal{H} \mid a_4 = a_6 = a_8 = a_{10} = a_{12} = 0, a_{14} \neq 0 \}$. For $f \in \mathcal{H}_1$, $\text{Res}(f, f') = 7^7a_{14}^6$. We have $|\mathcal{H}_1| = q - 1$. For $f \in \mathcal{H}_1$, by (4), in the stabilizer $G_f$ at $f$ we have $x^{14} = 1$, i.e., $G_f \cong G_{14} = \{ x \in \mathbb{F}_q^* \mid x^{14} = 1 \}$. And

$$
|G_{14}| = \gcd(q - 1, 14) = \begin{cases} 
14 & \text{if } 7 \mid (q - 1), \\
2 & \text{if } 7 \nmid (q - 1).
\end{cases}
$$

Define $\mathcal{H}_2 = \{ f \in \mathcal{H} \mid a_4 = a_6 = a_8 = a_{10} = a_{14} = 0, a_{12} \neq 0 \}$. For $f \in \mathcal{H}_2$, $f(u) = u^7 + a_{12}u = uf_1(u)$, $f_1(u) = u^8 + a_{12}$, $\text{Res}(f_1, f'_1) = 6^4a_{12}^5$. Hence we have

$$
|\mathcal{H}_2| = \begin{cases} 
0 & \text{if char}(\mathbb{F}_q) = 3, \\
q - 1 & \text{if char}(\mathbb{F}_q) \neq 3.
\end{cases}
$$

For $f \in \mathcal{H}_2$, by (4), we have $G_f \cong G_{12} = \{ x \in \mathbb{F}_q^* \mid x^{12} = 1 \}$. For the order of $G_{12}$, we have $|G_{12}| = \gcd(q - 1, 12)$, i.e.,

| $G_{12}$ | 4 | (q - 1) | 4 | (q - 1) |
|---|---|---|---|
| 3 | (q - 1) | 12 | 6 |
| 3 | (q - 1) | 4 | 2 |

Define $\mathcal{H}_3 = \{ f \in \mathcal{H} \mid a_4 = a_6 = a_{10} = a_{14} = 0, a_8 \neq 0, a_{12} \neq 0 \}$. For $f \in \mathcal{H}_3$, $f(u) = u^7 + a_8u^3 + a_{12}u = uf_1(u)$, $f_1(u) = u^6 + a_8u^2 + a_{12}$, $\text{Res}(f_1, f'_1) = 2^6a_{12}(4a_8^3 + 27a_{12}^2)^2$. Hence we have

$$
|\mathcal{H}_3| = \begin{cases} 
(q - 1)^2 & \text{if char}(\mathbb{F}_q) = 3, \\
(q - 1)(q - 2) & \text{if char}(\mathbb{F}_q) \neq 3.
\end{cases}
$$

And the stabilizer is $G_f \cong G_4 = \{ x \in \mathbb{F}_q^* \mid x^4 = 1 \}$,

$$
|G_4| = \gcd(q - 1, 4) = \begin{cases} 
4 & \text{if } 4 \mid (q - 1), \\
2 & \text{if } 4 \nmid (q - 1).
\end{cases}
$$
Define $\mathcal{H}_4 = \{ f \in \mathcal{H} \mid a_4 = a_8 = a_{10} = a_{14} = 0, a_6 \neq 0, a_{12} \neq 0 \}$. For $f \in \mathcal{H}_4$, $f(u) = u^7 + a_6 u^4 + a_{12} u = uf_1(u)$, $f_1(u) = u^6 + a_6 u^3 + a_{12}$, $\text{Res}(f_1, f'_1) = 3^6 a_{12}^2 (4a_{12} - a_6)^3$. Hence we have

$$|\mathcal{H}_4| = \begin{cases} 0 & \text{if } \text{char}(\mathbb{F}_q) = 3, \\ (q - 1)(q - 2) & \text{if } \text{char}(\mathbb{F}_q) \neq 3. \end{cases}$$

And the stabilizer is $G_f \cong G_6 = \{ \alpha \in \mathbb{F}_q^* \mid \alpha^6 = 1 \}$,

$$|G_6| = \gcd(q - 1, 6) = \begin{cases} 6 & \text{if } 3 \mid (q - 1), \\ 2 & \text{if } 3 \nmid (q - 1). \end{cases}$$

Define $\mathcal{H}_5 = \{ f \in \mathcal{H} \mid a_6 = a_8 = a_{10} = a_{14} = 0, a_4 \neq 0, a_{12} \neq 0 \}$. For $f \in \mathcal{H}_5$, $f(u) = u^7 + a_4 u^5 + a_{12} u = uf_1(u)$, $f_1(u) = u^6 + a_4 u^4 + a_{12}$, $\text{Res}(f_1, f'_1) = 2^6 a_{12}^2 (4a_4^3 + 27a_{12})^2$. Hence we have

$$|\mathcal{H}_5| = \begin{cases} (q - 1)^2 & \text{if } \text{char}(\mathbb{F}_q) = 3, \\ (q - 1)(q - 2) & \text{if } \text{char}(\mathbb{F}_q) \neq 3. \end{cases}$$

And the stabilizer is $G_f \cong G_4$.

Define $\mathcal{H}_6 = \{ f \in \mathcal{H} \mid a_6 = a_{10} = a_{14} = 0, a_4 \neq 0, a_8 \neq 0, a_{12} \neq 0 \}$. For $f \in \mathcal{H}_6$, $f(u) = u^7 + a_4 u^5 + a_8 u^3 + a_{12} u = uf_1(u)$, $f_1(u) = u^6 + a_4 u^4 + a_8 u^2 + a_{12}$, $f_1(u) = g(u^2)$, $g(u) = u^3 + a_4 u^2 + a_8 u + a_{12}$. Since $\text{char}(\mathbb{F}_q) \neq 2$, $f$ is separable if and only if $g$ is separable. By Proposition 3.5 we have

$$|\mathcal{H}_6| = \begin{cases} (q - 1)(q^2 - 3q + 3) & \text{if } \text{char}(\mathbb{F}_q) = 3, \\ (q - 1)(q^2 - 3q + 4) & \text{if } \text{char}(\mathbb{F}_q) \neq 3. \end{cases}$$

And the stabilizer is $G_f \cong G_4$.

**Theorem 4.1.** Suppose $\text{char}(\mathbb{F}_q) \neq 2, 7$. Let $N$ denote the number of isomorphism classes of hyperelliptic curves of genus $g = 3$ over $\mathbb{F}_q$, then we have: when $\text{char}(\mathbb{F}_q) = 3$,

<table>
<thead>
<tr>
<th>$N$</th>
<th>$7 \mid (q - 1)$</th>
<th>$7 \nmid (q - 1)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$4 \mid (q - 1)$</td>
<td>$2q^5 + 2q^2 - 2q + 14$</td>
<td>$2q^5 + 2q^2 - 2q + 2$</td>
</tr>
<tr>
<td>$4 \nmid (q - 1)$</td>
<td>$2q^5 + 12$</td>
<td>$2q^5$</td>
</tr>
</tbody>
</table>
when \( \text{char}(\mathbb{F}_q) \neq 3 \),

| \( \mathcal{H}_i \) | \( | \mathcal{H}_i | \) |
|-----------------|-----------------|
| \( \mathcal{H}_1 \) | \( q - 1 \) |
| \( \mathcal{H}_2 \) | \( 0 \) |
| \( \mathcal{H}_3 \) | \( (q - 1)^2 \) |
| \( \mathcal{H}_4 \) | \( 0 \) |
| \( \mathcal{H}_5 \) | \( (q - 1)^2 \) |
| \( \mathcal{H}_6 \) | \( (q - 1)(q^2 - 3q + 3) \) |
| \( \mathcal{H}_7 \) | \( (q - 1)(q^5 - q^2 + q - 2) \) |

Thus

\[
N = \frac{|\mathcal{H}_1|}{(G : G_{14})} + \frac{|\mathcal{H}_2|}{(G : G_{12})} + \frac{|\mathcal{H}_3|}{(G : G_4)} + \frac{|\mathcal{H}_4|}{(G : G_{6})} + \frac{|\mathcal{H}_5|}{(G : G_4)} + \frac{|\mathcal{H}_6|}{(G : G_4)} + \frac{|\mathcal{H}_7|}{(G : G_2)}.
\]

**Proof.** Notations \( \mathcal{H}, \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3, \mathcal{H}_4, \mathcal{H}_5, \mathcal{H}_6 \) are the same as above, define \( \mathcal{H}_7 = \mathcal{H} - \bigcup_{i=1}^{6} \mathcal{H}_i \). Then we have a disjoint union

\[
\mathcal{H} = \bigcup_{i=1}^{7} \mathcal{H}_i.
\]

For \( f \in \mathcal{H} \), \( f(u) = u^7 + a_4u^4 + a_6u^6 + a_8u^8 + a_{10}u^{10} + a_{12}u + a_{14} \), since \( f \) has no multiple roots, \( a_{12}, a_{14} \) are not all zeros. Analyzing the coefficients \( a_4, a_6, a_8, a_{10}, a_{12}, a_{14} \) as \( 0 \) and different from \( 0 \), by (4) it is easy to see that we have \( G_f \cong G_2 = \{ x \in \mathbb{F}_q^* \mid x^2 = 1 \} \) for \( f \) in \( \mathcal{H}_7 \), and \( |G_2| = \gcd(q - 1, 2) = 2 \). From \( |\mathcal{H}_7| = |\mathcal{H}| - \sum_{i=1}^{6} |\mathcal{H}_i| = q^6 - q^5 - \sum_{i=1}^{6} |\mathcal{H}_i| \) and the preceding analysis we have

\[
G_f
\]

Thus

\[
N = \frac{|\mathcal{H}_1|}{(G : G_{14})} + \frac{|\mathcal{H}_2|}{(G : G_{12})} + \frac{|\mathcal{H}_3|}{(G : G_4)} + \frac{|\mathcal{H}_4|}{(G : G_{6})} + \frac{|\mathcal{H}_5|}{(G : G_4)} + \frac{|\mathcal{H}_6|}{(G : G_4)} + \frac{|\mathcal{H}_7|}{(G : G_2)}.
\]
When \( \text{char}(\mathbb{F}_q) = 3 \),

\[
N = |G_{14}| + (q - 1)|G_4| + (q - 1)|G_4| + (q^2 - 3q + 3)|G_4| + (q^5 - q^2 + q - 2) \cdot 2
\]
\[
= 2(q^5 - q^2 + q - 2) + (q^2 - q + 1)|G_4| + |G_{14}|
\]

we get the corresponding consequences in the theorem.

When \( \text{char}(\mathbb{F}_q) \neq 3 \),

\[
N = |G_{14}| + |G_{12}| + (q - 2)|G_4| + (q - 2)|G_6| + (q - 2)|G_4|
\]
\[
+ (q^2 - 3q + 4)|G_4| + 2(q^5 - q^2)
\]
\[
= 2(q^5 - q^2) + |G_{14}| + |G_{12}| + (q - 2)|G_6| + (q^2 - q)|G_4|
\]

we get the corresponding consequences in the theorem.

\[\square\]

Remark. Jeong [11] also obtained the formula in this case (see [11, Theorem 3.4]), but his result did not distinguish two cases: \( \text{char}(\mathbb{F}_q) = 3 \) and \( \text{char}(\mathbb{F}_q) \neq 3 \). If \( \text{char}(\mathbb{F}_q) = 3 \), then \( q \equiv 3 \pmod{12} \) or \( q \equiv 9 \pmod{12} \). But in the table of [11, Theorem 3.4] or in the Table 3 of [4, p. 601], they only consider the cases: \( q \equiv 1, 5, 7, 11 \pmod{12} \). Hence their results are incomplete. The reason is that when \( \text{char}(\mathbb{F}_q) = 3 \), the computation of \( |H_3| \) in the Lemma 3.3 of [11] is incorrect. Seeing the proof of Lemma 3.3 of [11], in (3), we have \( \Delta(f) = 0 \). Hence the correct value of \( |H_3| \) is zero.

5. \( \text{Char}(\mathbb{F}_q) = 7 \)

First we introduce a useful lemma.

**Lemma 5.1** (Lidl and Niederreiter [13]). Suppose \( \mathbb{F}_{q^d} \) is an extension field of \( \mathbb{F}_q \), \( a \in \mathbb{F}_{q^d} \), then the equation \( X^{q^d} - X = a \) has a solution in \( \mathbb{F}_{q^d} \) if and only if \( \text{Tr}_{q^d/q}(a) = 0 \), where \( \text{Tr}_{q^d/q} \) is the trace mapping from \( \mathbb{F}_{q^d} \) onto \( \mathbb{F}_q \).

**Corollary 5.2.** Suppose \( a \in \mathbb{F}_{q^d}^*, b \in \mathbb{F}_{q^d} \), then the equation \( X^{q^d} - a^{q-1}X = b \) has a solution in \( \mathbb{F}_{q^d} \) if and only if

\[
\text{Tr}_{q^d/q} \left( \frac{b}{a^{q-1}} \right) = 0.
\]

**Proof.** We divide the two sides of the equation by \( a^q \),

\[
\left( \frac{X}{a} \right)^q - \frac{X}{a} = \frac{b}{a^q},
\]

now it follows from Lemma 5.1. \( \square \)
Below suppose \( \text{char}(\mathbb{F}_q) = 7 \), say \( q = 7^m, m > 0 \). Now (1) turns into

\[
\begin{align*}
\begin{cases}
\varepsilon \overline{a}_1 = 2\gamma + a_1, \\
\varepsilon^3 \overline{a}_3 = 2\delta + 3\beta a_1 + a_3, \\
\varepsilon^5 \overline{a}_5 = 2\theta + 3\beta^2 a_1 + 2\beta a_3 + a_5, \\
\varepsilon^7 \overline{a}_7 = 2\varepsilon + \beta^3 a_1 + \beta^2 a_3 + \beta a_5 + a_7, \\
\varepsilon^2 \overline{a}_2 = 6\gamma^2 + 6\gamma a_1 + a_2, \\
\varepsilon^4 \overline{a}_4 = 5\gamma \delta + (6\delta + 4\beta \varepsilon) a_1 + 6\beta a_2 + 6\gamma a_3 + a_4, \\
\varepsilon^6 \overline{a}_6 = 6\delta^2 + 5\gamma \theta + (6\delta + 4\delta \varepsilon^2 + 4\beta^2 \gamma) a_1 + \beta^2 a_2 + (6\delta + 5\beta \gamma) a_3 + 5\beta a_4 + 6\gamma a_5 + a_6, \\
\varepsilon^8 \overline{a}_8 = 5\gamma \varepsilon + 5\delta \theta + (6\varepsilon + 4\beta \theta + 4\beta^2 \delta + 6\beta^3 \gamma) a_1 + 6\beta^3 a_2 + (6\delta + 5\beta \delta + 6\beta^2 \delta) a_3 + 3\beta \delta a_4 + 6\delta a_7 + 3\delta a_8 + a_{10}, \\
\varepsilon^{10} \overline{a}_{10} = 6\theta^2 + 5\delta \varepsilon + (4\theta \varepsilon + 4\beta^2 \theta + 6\delta \delta) a_1 + \beta^4 a_2 + (6\varepsilon + 5\beta \theta + 6\beta^2 \delta) a_3 + 3\beta \delta a_4 + 6\delta a_7 + 3\delta a_8 + a_{10}, \\
\varepsilon^{12} \overline{a}_{12} = 5\varepsilon + (4\varepsilon^2 + 6\beta^2 \theta) a_1 + 6\beta^3 a_2 + (5\beta \varepsilon + 6\beta^2 \theta) a_3 + 5\beta^4 a_4 + (6\varepsilon + 6\beta \theta) a_5 + 4\beta^3 a_6 + 6\delta a_7 + 3\beta^2 a_8 + 2\beta a_{10} + a_{12}, \\
\varepsilon^{14} \overline{a}_{14} = \beta^6 + 6\varepsilon^2 + 6\beta^3 \varepsilon a_1 + \beta^6 a_2 + 6\beta^2 \varepsilon a_3 + \beta^5 a_4 + 6\beta \varepsilon a_5 + \beta^4 a_6 + 6\varepsilon a_7 + \beta^3 a_8 + \beta^2 a_{10} + \beta a_{12} + a_{14}.
\end{cases}
\end{align*}
\]

By (5), we can choose \( \gamma, \delta, \theta, \varepsilon \) for which \( \overline{a}_1 = \overline{a}_3 = \overline{a}_5 = \overline{a}_7 = 0 \). Hence we can assume \( a_1 = a_3 = a_5 = a_7 = 0 \), the Weierstrass equation is

\[
v^2 = u^7 + a_2 u^6 + a_4 u^5 + a_6 u^4 + a_8 u^3 + a_{10} u^2 + a_{12} u + a_{14}.
\]

By (5), in the coordinate transformation between two Weierstrass equations of form (6) \( (a_i = \overline{a}_i = 0, i = 1, 3, 5, 7) \), we must have \( \gamma = \delta = \theta = \varepsilon = 0 \). The coordinate transformation is

\[
(u, v) \mapsto (x^2 u + \beta, x^7 v), \quad x \in \mathbb{F}_q^*, \quad \beta \in \mathbb{F}_q.
\]

Now (5) turns into

\[
\begin{align*}
\begin{cases}
x^2 \overline{a}_2 = a_2, \\
x^3 \overline{a}_3 = 6\beta a_2 + a_4, \\
x^6 \overline{a}_6 = \beta^2 a_2 + 5\beta a_4 + a_6, \\
x^8 \overline{a}_8 = 6\beta^3 a_2 + 3\beta^2 a_4 + 4\beta a_6 + a_8, \\
x^{10} \overline{a}_{10} = \beta^4 a_2 + 3\beta^3 a_4 + 6\beta^2 a_6 + 3\beta a_8 + a_{10}, \\
x^{12} \overline{a}_{12} = 6\beta^5 a_2 + 5\beta^4 a_4 + 4\beta^3 a_6 + 3\beta^2 a_8 + 2\beta a_{10} + a_{12}, \\
x^{14} \overline{a}_{14} = \beta^7 + \beta^6 a_2 + \beta^5 a_4 + \beta^4 a_6 + \beta^3 a_8 + \beta^2 a_{10} + \beta a_{12} + a_{14}.
\end{cases}
\end{align*}
\]

Below we will consider the reduced forms of (6). By choosing appropriate transformations, we can transform the Weierstrass equations into the following reduced
forms:

\[ v^2 = u^7 + a_2 u^6 + a_6 u^4 + a_8 u^3 + a_{10} u^2 + a_{12} u + a_{14}, \quad a_2 \neq 0, \quad (9) \]

\[ v^2 = u^7 + a_4 u^5 + a_8 u^3 + a_{10} u^2 + a_{12} u + a_{14}, \quad a_4 \neq 0, \quad (10) \]

\[ v^2 = u^7 + a_6 u^4 + a_{10} u^2 + a_{12} u + a_{14}, \quad a_6 \neq 0, \quad (11) \]

\[ v^2 = u^7 + a_8 u^3 + a_{12} u + a_{14}, \quad a_8 \neq 0, \quad (12) \]

\[ v^2 = u^7 + a_{10} u^2 + a_{14}, \quad a_{10} \neq 0, \quad (13) \]

\[ v^2 = u^7 + a_{12} u + a_{14}, \quad (14) \]

**Proposition 5.3.** The Weierstrass equation (6) is equivalent to unique one in (9)–(14).

**Proof.** See [4, Theorem 5.1]. □

Now we will compute the number of isomorphism classes of hyperelliptic curves whose Weierstrass equation is of form (9)–(14). Starting with the simplest one.

**Proposition 5.4.** Define \( H_6 = \{ f(u) = u^7 + a_{12} u + a_{14} \mid f \text{ is separable} \} \). Let \( N_6 \) denote the number of isomorphism classes of hyperelliptic curves of form (14). Then we have \( |H_6| = q(q - 1) \),

\[ N_6 = \begin{cases} 
14 & \text{if } m \text{ is even}, \\
8 & \text{if } m \text{ is odd}. 
\end{cases} \]

**Proof.** See the proof of [4, Theorem 5.5]. □

**Proposition 5.5.** Define \( H_5 = \{ f(u) = u^7 + a_{10} u^2 + a_{14} \mid a_{10} \neq 0, f \text{ is separable} \} \). Let \( N_5 \) denote the number of isomorphism classes of hyperelliptic curves of form (13). Then we have \( |H_5| = (q - 1)^2, N_5 = 2q - 2 \).

**Proof.** See the proof of [4, Theorem 5.5]. □

**Proposition 5.6.** Define \( H_4 = \{ f(u) = u^7 + a_8 u^3 + a_{12} u + a_{14} \mid a_8 \neq 0, f \text{ is separable} \} \). Let \( N_4 \) denote the number of isomorphism classes of hyperelliptic curves of form (12). Then we have \( |H_4| = q(q - 1)^2 \),

\[ N_4 = \begin{cases} 
2(q^2 - 2), & \text{if } m \text{ is even}, \\
2q(q - 1), & \text{if } m \text{ is odd}. 
\end{cases} \]

**Proof.** See the proof of [4, Theorem 5.5]. □
**Proposition 5.7.** Define \( \mathcal{H}_3 = \{ f(u) = u^7 + a_6u^4 + a_{10}u^2 + a_{14} \mid a_6 \neq 0, f \) is separable \}. Let \( N_3 \) denote the number of isomorphism classes of hyperelliptic curves of form \((11)\). Then we have that \( |\mathcal{H}_3| = (q - 1)(q^3 - q^2 - 1) \) and \( N_3 = 2q^3 - 2q^2 + 4q - 10 \).

**Proof.** See the proof of \([4, \text{Theorem 5.5}]\). \(\Box\)

**Proposition 5.8.** Define \( \mathcal{H}_2 = \{ f(u) = u^7 + a_4u^5 + a_8u^3 + a_{12}u + a_{14} \mid a_4 \neq 0, f \) is separable \}. Let \( N_2 \) denote the number of isomorphism classes of hyperelliptic curves of form \((10)\). Then we have

\[
N_2 = \begin{cases} 
\frac{2|\mathcal{H}_2|}{q - 1} + 2(q^2 - 2q + 2) & \text{if } m \text{ is even,} \\
\frac{2|\mathcal{H}_2|}{q - 1} & \text{if } m \text{ is odd.}
\end{cases}
\]

**Proof.** Now \((8)\) turns into (necessarily \( \beta = 0 \))

\[
\begin{align*}
  x^4u_4 &= a_4, \\
  x^8u_8 &= a_8, \\
  x^{10}u_{10} &= a_{10}, \\
  x^{12}u_{12} &= a_{12}, \\
  x^{14}u_{14} &= a_{14}.
\end{align*}
\]

Define \( \mathcal{H}_{21} = \{ f \in \mathcal{H}_2 \mid a_{10} = a_{14} = 0 \} \). For \( f \in \mathcal{H}_{21} \), \( f(u) = u^7 + a_4u^5 + a_8u^3 + a_{12}u = u f_1(u) \), \( f_1(u) = u^6 + a_4u^4 + a_8u^2 + a_{12} \). \( f_1(u) = g(u^2) \), \( g(u) = u^3 + a_4u^2 + a_8u + a_{12} \). \( f \) is separable \( \iff a_{12} \neq 0 \) and \( f_1 \) is separable \( \iff a_{12} \neq 0 \) and \( g \) is separable. By Proposition 3.5,

\[
|\mathcal{H}_{21}| = L_4 + L_6 = (q - 1)(q - 2) + (q - 1)(q^2 - 3q + 4) = (q - 1)(q^2 - 2q + 2).
\]

And the size of the stabilizer is

\[
|G_f| = \gcd(q - 1, 4) = \begin{cases} 4 & \text{if } m \text{ is even,} \\
2 & \text{if } m \text{ is odd.}
\end{cases}
\]

Thus, the number of orbits contained in \( \mathcal{H}_{21} \) is

\[
\begin{cases} 
\frac{(q - 1)(q^2 - 2q + 2)}{(q - 1)/4} = 4(q^2 - 2q + 2) & \text{if } m \text{ is even,} \\
\frac{(q - 1)(q^2 - 2q + 2)}{(q - 1)/2} = 2(q^2 - 2q + 2) & \text{if } m \text{ is odd.}
\end{cases}
\]
Define $\mathcal{H}_{22} = \{ f \in \mathcal{H}_2 \mid a_{10}, a_{14} \text{ are not all } 0 \}. \text{ For } f \in \mathcal{H}_{22}, \text{ the size of the stabilizer is } |G_f| = 2. \text{ Thus, the number of orbits contained in } \mathcal{H}_{22} \text{ is }

$$
\frac{|\mathcal{H}_2| - (q - 1)(q^2 - 2q + 2)}{(q - 1)/2} = \frac{2|\mathcal{H}_2|}{q - 1} - 2(q^2 - 2q + 2).
$$

So

$$
N_2 = \begin{cases} 
4(q^2 - 2q + 2) + \frac{2|\mathcal{H}_2|}{q - 1} - 2(q^2 - 2q + 2) & \text{if } m \text{ is even,} \\
2(q^2 - 2q + 2) + \frac{2|\mathcal{H}_2|}{q - 1} - 2(q^2 - 2q + 2) & \text{if } m \text{ is odd.} 
\end{cases}
$$

**Proposition 5.9.** Define $\mathcal{H}_1 = \{ f(u) = u^7 + a_2u^6 + a_6u^4 + a_8u^3 + a_{10}u^2 + a_{12}u + a_{14} \mid a_2 \neq 0, f \text{ is separable} \}. \text{ Let } N_1 \text{ denote the number of isomorphism classes of hyperelliptic curves of form (9). Then we have that } |\mathcal{H}_1| = \frac{1}{2}q(q - 1)(2q^4 - 2q^3 + 1) \text{ and } N_1 = 2q^5 - 2q^4 + q.

**Proof.** See the proof of [4, Theorem 5.5]. □

**Lemma 5.10.** With the notations $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$ be as above, then we have

$$
|\mathcal{H}_1| + |\mathcal{H}_2| + |\mathcal{H}_3| = q^2(q - 1)^2(q^2 + q + 1).
$$

**Proof.** Define $\mathcal{W} = \{ f(u) = u^7 + a_2u^6 + a_4u^5 + a_6u^4 + a_8u^3 + a_{10}u^2 + a_{12}u + a_{14} \in \mathbb{F}_q[u] \mid f \text{ is separable} \}. \text{ By Theorem 3.1 we have } |\mathcal{W}| = q^7 - q^6. \text{ Define } \mathcal{W}_1 = \{ f \in \mathcal{W} \mid a_2 \neq 0 \} \text{ and } \mathcal{W}_2 = \{ f \in \mathcal{W} \mid a_2 = 0 \}. \text{ Then we have a disjoint union } \mathcal{W} = \mathcal{W}_1 \cup \mathcal{W}_2.

Define $\mathcal{W}_{11} = \{ f \in \mathcal{W}_1 \mid a_4 \neq 0 \}$ and $\mathcal{W}_{12} = \{ f \in \mathcal{W}_1 \mid a_4 = 0 \}. \text{ We have } \mathcal{W}_{12} = \mathcal{H}_1. \text{ Thus we have a disjoint union } \mathcal{W}_1 = \mathcal{W}_{11} \cup \mathcal{W}_{12}. \text{ For } f \in \mathcal{W}_1, \text{ it is easy to see } f(u + \frac{a_4}{a_2}) \in \mathcal{W}_{12}. \text{ Using a similar method proving Proposition 3.4, we have }

$$
|\mathcal{W}_1| = q|\mathcal{W}_{12}| = q|\mathcal{H}_1|.
$$

Define $\mathcal{W}_{21} = \{ f \in \mathcal{W}_2 \mid a_4 \neq 0 \}$ and $\mathcal{W}_{22} = \{ f \in \mathcal{W}_2 \mid a_4 = 0 \}. \text{ We have a disjoint union } \mathcal{W}_2 = \mathcal{W}_{21} \cup \mathcal{W}_{22}. \text{ Define } \mathcal{W}_{211} = \{ f \in \mathcal{W}_{21} \mid a_6 \neq 0 \} \text{ and } \mathcal{W}_{212} = \{ f \in \mathcal{W}_{21} \mid a_6 = 0 \}. \text{ } \mathcal{W}_{212} \text{ is just } \mathcal{H}_2. \text{ Similarly, we have }

$$
|\mathcal{W}_{21}| = q|\mathcal{H}_2|.
$$
Define $W_{221} = \{ f \in W_2 \mid a_6 \neq 0 \}$ and $W_{222} = \{ f \in W_2 \mid a_6 = 0 \}$. Define $W_{2211} = \{ f \in W_{221} \mid a_8 \neq 0 \}$ and $W_{2212} = \{ f \in W_{221} \mid a_8 = 0 \}$. $W_{2212}$ is just $H_3$. Similarly, we have

$$|W_{221}| = q|H_3|.$$

Define $W_{2221} = \{ f \in W_{222} \mid a_8 \neq 0 \}$ and $W_{2222} = \{ f \in W_{222} \mid a_8 = 0 \}$. Define $W_{22211} = \{ f \in W_{2221} \mid a_{10} \neq 0 \}$ and $W_{22212} = \{ f \in W_{2221} \mid a_{10} = 0 \}$. $W_{22212}$ is just $H_4$. By Proposition 5.6 we have

$$|W_{2221}| = q|W_{22212}| = q|H_4| = q^2(q - 1)^2.$$

Define $W_{22221} = \{ f \in W_{2222} \mid a_{10} \neq 0 \}$ and $W_{22222} = \{ f \in W_{2222} \mid a_{10} = 0 \}$. $W_{22222}$ is just $H_6$. By Proposition 5.4 we have $|W_{22222}| = q(q - 1)$.

Define $W_{222211} = \{ f \in W_{22221} \mid a_{12} \neq 0 \}$ and $W_{222212} = \{ f \in W_{22221} \mid a_{12} = 0 \}$. $W_{222212}$ is just $H_5$. By Proposition 5.5 we have $|W_{222212}| = (q - 1)^2$. Thus, we have

$$|W_{22221}| = q|W_{222212}| = q(q - 1)^2.$$

Since we have a disjoint union

$$W = W_1 \cup W_21 \cup W_{221} \cup W_{2221} \cup W_{22221} \cup W_{22222},$$

taking the cardinalities of the two sides, we get

$$q^7 - q^6 = q|H_1| + q|H_2| + q|H_3| + q^2(q - 1)^2 + q(q - 1)^2 + q(q - 1).$$

Hence

$$|H_1| + |H_2| + |H_3| = q^2(q - 1)^2(q^2 + q + 1). \quad \square$$

**Corollary 5.11.** We have that $|H_2| = \frac{1}{2}(q - 1)(2q^4 - 2q^3 - q + 2)$ and

$$N_2 = \begin{cases} 2q^4 - 2q^3 + 2q^2 - 5q + 6 & \text{if } m \text{ is even,} \\ 2q^4 - 2q^3 - q + 2 & \text{if } m \text{ is odd.} \end{cases}$$

**Proof.** The value of $|H_2|$ follows from Propositions 5.4–5.7, 5.9 and Lemma 5.10. The value of $N_2$ follows from Proposition 5.8. $\square$
**Theorem 5.12.** Let \( N \) denote the number of isomorphism classes of hyperelliptic curves of genus 3 over \( \mathbb{F}_q(q = 7^m, m > 0) \), then we have

\[
N = \begin{cases} 
2q^5 + 2q^2 + 2q + 4 & \text{if } m \text{ is even}, \\
2q^5 + 4q - 2 & \text{if } m \text{ is odd}.
\end{cases}
\]

**Proof.** It follows from Propositions 5.4–5.7, 5.9 and Corollary 5.11. \( \square \)

**Remark.** The value of \( N_2 \) has only been bounded in [4, Theorem 5.5]. The bounds of \( N \) given in [4, Theorem 5.5] are very close to our exact values.

**6. Char(\( \mathbb{F}_q \)) = 2**

In this section we suppose \( \text{char}(\mathbb{F}_q) = 2 \), say \( q = 2^m, m > 0 \). Now (1) turns into

\[
\begin{align*}
\varepsilon \overline{a}_1 &= a_1, \\
\varepsilon^3 \overline{a}_3 &= \beta a_1 + a_3, \\
\varepsilon^5 \overline{a}_5 &= \beta^2 a_1 + a_5, \\
\varepsilon^7 \overline{a}_7 &= \beta^3 a_1 + \beta^2 a_3 + \beta a_5 + a_7, \\
\varepsilon^2 \overline{a}_2 &= \beta + \gamma^2 + \gamma a_1 + a_2, \\
\varepsilon^4 \overline{a}_4 &= \beta^2 + (\delta + \beta \gamma) a_1 + \gamma a_3 + a_4, \\
\varepsilon^6 \overline{a}_6 &= \beta^3 + \delta^2 + (\theta + \beta \delta + \beta^2 \gamma) a_1 + \beta^2 a_2 \\
&\quad + \delta a_3 + \beta a_4 + \gamma a_5 + a_6, \\
\varepsilon^8 \overline{a}_8 &= \beta^4 + (\epsilon + \beta \theta + \beta^2 \delta + \beta^3 \gamma) a_1 + (\theta + \beta^2 \gamma) a_3 \\
&\quad + (\delta + \beta \gamma) a_5 + \gamma a_7 + a_8, \\
\varepsilon^{10} \overline{a}_{10} &= \beta^5 + \theta^2 + (\beta \epsilon + \beta^2 \theta + \beta^3 \delta) a_1 + \beta^4 a_2 + (\epsilon + \beta^2 \delta) a_3 \\
&\quad + (\theta + \beta \delta) a_5 + \delta a_7 + \beta a_8 + a_{10}, \\
\varepsilon^{12} \overline{a}_{12} &= \beta^6 + (\beta^2 \epsilon + \beta^3 \theta) a_1 + \beta^2 \theta a_3 + \beta^4 a_4 \\
&\quad + (\epsilon + \beta \theta) a_5 + \theta a_7 + \beta^2 a_8 + a_{12}, \\
\varepsilon^{14} \overline{a}_{14} &= \beta^7 + \epsilon^2 + \beta^3 \epsilon a_1 + \beta^6 a_2 + \beta^2 \epsilon a_3 + \beta^5 a_4 + \beta \epsilon a_5 + \beta^4 a_6 \\
&\quad + \epsilon a_7 + \beta^3 a_8 + \beta^2 a_{10} + \beta a_{12} + a_{14}.
\end{align*}
\]

Since \( a_1, a_3, a_5, a_7 \) are not all zeros, by (15) we can divide hyperelliptic curves into four types:

- **Type I:** \( a_1 \neq 0 \).
- **Type II:** \( a_1 = 0, a_3 \neq 0 \).
- **Type III:** \( a_1 = a_3 = 0, a_5 \neq 0 \).
- **Type IV:** \( a_1 = a_3 = a_5 = 0, a_7 \neq 0 \).

Below we consider each type separably.
6.1. Type I: $a_1 \neq 0$

Suppose $a_1 \neq 0$. Putting $\alpha = a_1$, by the first formula of (15), we have $\bar{a}_1 = 1$. So we can suppose $a_1 = 1$.

Again putting

$$\begin{align*}
\beta &= a_3, \\
\delta &= \beta^2 + \beta \gamma + \gamma a_3 + a_4, \\
\theta &= \beta^3 + \delta^2 + \beta \delta + \beta^2 \gamma + \beta^2 a_2 + \delta a_3 + \beta a_4 + \gamma a_5 + a_6, \\
\epsilon &= \beta^4 + \beta \theta + \beta^2 \delta + \beta^3 \gamma + (\theta + \beta^2 \gamma)a_3 + (\delta + \beta \gamma)a_5 + \gamma a_7 + a_8,
\end{align*}$$

by (15), we have $\bar{a}_3 = \bar{a}_4 = \bar{a}_6 = \bar{a}_8 = 0$. So we can suppose $a_3 = a_4 = a_6 = a_8 = 0$.

Now the Weierstrass equation turns into

$$v^2 + (u^3 + a_5 u + a_7)v = u^7 + a_2 u^6 + a_{10} u^2 + a_{12} u + a_{14}.$$  \hfill (16)

And (15) turns into

$$\begin{align*}
\bar{a}_5 &= a_5, \\
\bar{a}_7 &= a_7, \\
\bar{a}_2 &= \gamma^2 + \gamma + a_2, \\
\bar{a}_{10} &= \theta^2 + \theta a_5 + a_{10}, \\
\bar{a}_{12} &= \epsilon a_5 + \theta a_7 + a_{12}, \\
\bar{a}_{14} &= \epsilon^2 + \epsilon a_7 + a_{14}
\end{align*}$$

and

$$\begin{align*}
\alpha &= 1, \\
\beta &= 0, \\
\delta &= 0, \\
0 &= \theta + \gamma a_5, \\
0 &= \epsilon + \gamma a_7.
\end{align*}$$

That is,

$$\begin{align*}
\bar{a}_5 &= a_5, \\
\bar{a}_7 &= a_7, \\
\bar{a}_2 &= \gamma^2 + \gamma + a_2, \\
\bar{a}_{10} &= (\gamma^2 + \gamma)a_5^2 + a_{10}, \\
\bar{a}_{12} &= a_{12}, \\
\bar{a}_{14} &= (\gamma^2 + \gamma)a_7^2 + a_{14}
\end{align*}$$ \hfill (17)

Thus the coordinate transformation is determined by $\gamma$, the group of the coordinate transformation is $G \cong \mathbb{F}_q$, its order is $|G| = q$. And by (17) it is easy to see that the
stabilizer consists of $\gamma = 0, 1$, its size is 2. Hence to decide the number of isomorphism classes of hyperelliptic curves of form (16), it must decide the number of hyperelliptic curves of form (16).

**Proposition 6.1.** Let $N_1$ denote the number of isomorphism classes of hyperelliptic curves of form (16), then the number of hyperelliptic curves of form (16) is $q^6 - q^5$, and

$$N_1 = 2q^5 - 2q^4.$$

**Proof.** The Weierstrass equation (16) represents a hyperelliptic curve if and only if there are no $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ satisfying

$$\begin{cases}
y^2 = f(x), \\
h(x) = 0, \\
yh'(x) = f'(x),
\end{cases}$$

(18)

where $h(u) = u^3 + a_5u + a_7$, $f(u) = u^7 + a_2u^6 + a_{10}u^2 + a_{12}u + a_{14}$.

Since $h'(u) = u^2 + a_5$, $f'(u) = u^6 + a_{12}$, we distinguish three cases:

Suppose $a_7 = a_5 = 0$. $h(x) = 0$ is just $x = 0$. Thus, $h'(x) = h'(0) = 0$, $f'(x) = f'(0) = a_{12}$. Now no solution of (18) is equivalent to $a_{12} \neq 0$. The number of hyperelliptic curves of this kind is $q^3(q - 1)$.

Suppose $a_7 = 0, a_5 \neq 0$. The equation $h(x) = 0$ has two solutions $x = 0, x^2 = a_5$. For $x = 0$, $h'(x) = a_5$, $f'(x) = a_{12}$. Now no solution of (18) is equivalent to $a_{12} \neq a_5^3$. So, for $a_7 = 0, a_5 \neq 0$, (16) represents a hyperelliptic curve if and only if

$$a_{12} \neq a_5^3, \quad a_{14} \neq \left(\frac{a_{12}}{a_5}\right)^2.$$

Thus, the number of hyperelliptic curves of this kind is $q^2(q - 1)^3$.

Suppose $a_7 \neq 0$. Now $h'(x) = x^2 + a_5 \neq 0$, no solution of (18) is equivalent to

$$\left(\frac{x^6 + a_{12}}{x^2 + a_5}\right)^2 \neq f(x), \text{ where } x^3 + a_5x + a_7 = 0.$$

An easy computation shows that this condition is just

$$a_{14} \neq (a_{10} + a_{2}a_7^2 + a_7^2 + a_7^{-2}(a_5^6 + a_{12}^2))x^2 + (a_5^2 + a_7^2 + a_{12})x + a_5^4 + a_2a_7^2,$$

(19)

where $x^3 + a_5x + a_7 = 0$. 
It is easy to see \( \text{Res}(h, h') = a_2^2 \neq 0 \), so \( h \) is separable. Considering the decomposition of \( h(u) \) over \( \mathbb{F}_q \), there are three cases:

Case (i): \( h(u) \) is irreducible over \( \mathbb{F}_q \). Because the number of monic irreducible polynomials of degree 3 over \( \mathbb{F}_q \), by Lemma 3.2, is \( \frac{1}{3}(q^3 - q) \). For the irreducible polynomial \( b(u) = u^3 + b_1u^2 + b_2u + b_3 \), it is easy to see that the polynomial \( b(u + b_1) \) is irreducible and the coefficient of \( u^2 \) is 0. Now using a method similar to the proof of Proposition 3.4, we know that the number of this kind of \( h(u) \) is

\[
\frac{1}{q} \cdot \frac{1}{3}(q^3 - q) = \frac{1}{3}(q^2 - 1).
\]

Hence \( h \) is the minimal polynomial of \( x \) over \( \mathbb{F}_q \).

Suppose \( a_{12} = a_3^2 + a_7^2, a_{10} = a_2a_5^2 + a_7^2 + a_7^{-2}(a_5^6 + a_{12}^2) = a_2a_5^2 \). Now (19) turns into

\[
a_{14} \neq a_5^4 + a_5^2a_7 + a_2a_7^2.
\]

The number of hyperelliptic curves of this kind is

\[
\frac{1}{3} (q^2 - 1) \cdot q \cdot 1 \cdot (q - 1) = \frac{1}{3} q(q - 1)^2(q + 1).
\]

Suppose \( a_{12} = a_3^2 + a_7^2, a_{10} \neq a_2a_5^2 + a_7^2 + a_7^{-2}(a_5^6 + a_{12}^2) = a_2a_5^2 \). Then (19) shows that \( a_{14} \) can be arbitrary. The number of hyperelliptic curves of this kind is

\[
\frac{1}{3} (q^2 - 1) \cdot q \cdot (q - 1) \cdot 1 \cdot q = \frac{1}{3} q^2(q - 1)^2(q + 1).
\]

Suppose \( a_{12} \neq a_3^2 + a_7^2, a_{10} = a_2a_5^2 + a_7^2 + a_7^{-2}(a_5^6 + a_{12}^2) \). Then (19) shows that \( a_{14} \) can be arbitrary. The number of hyperelliptic curves of this kind is

\[
\frac{1}{3} (q^2 - 1) \cdot q \cdot (q - 1) \cdot q = \frac{1}{3} q^2(q - 1)^2(q + 1).
\]

Suppose \( a_{12} \neq a_3^2 + a_7^2, a_{10} \neq a_2a_5^2 + a_7^2 + a_7^{-2}(a_5^6 + a_{12}^2) \). Then (19) shows that \( a_{14} \) can be arbitrary. The number of hyperelliptic curves of this kind is

\[
\frac{1}{3} (q^2 - 1) \cdot q \cdot (q - 1) \cdot q = \frac{1}{3} q^2(q - 1)^3(q + 1).
\]

Therefore, when \( h \) is irreducible over \( \mathbb{F}_q \), the number of hyperelliptic curves of form (16) is

\[
\frac{1}{3} q(q - 1)^2(q + 1) + \frac{1}{3} q^2(q - 1)^2(q + 1) + \frac{1}{3} q^2(q - 1)^2(q + 1) + \frac{1}{3} q^2(q - 1)^3(q + 1) = \frac{1}{3} q(q^2 - 1)(q^3 - 1).
\]
Case (ii): $h(u)$ decomposes over $\mathbb{F}_q$ as the product of one degree-1 polynomial and one irreducible degree-2 polynomial. That is $h(u) = u^3 + a_5 u + a_7 = (u^2 + au + b)(u + a), a, b \in \mathbb{F}_q$, and $u^2 + au + b$ is irreducible over $\mathbb{F}_q$. We have $a_5 = a^2 + b, a_7 = ab$.

The number of this kind of $h$ is $\frac{1}{2}(q^2 - q)$.

If $x = a$, then (19) turns into

$$a_{14} \neq (a_{10} + a_2 a_5^2 + a_2^2 + a_7^2 - (a_5^6 + a_12^2))a^2 + (a_3^3 + a_7^2 + a_{12})a + a_5^4 + a_5^2 a_7 + a_2 a_7^2. \quad (20)$$

If $x^2 + ax + b = 0$, then (19) turns into

$$a_{14} \neq (a_3^3 + a_7^2 + a_{12} + a a_{10} + a a_2 a_5^2 + a a_2^2 + a a_7 + a a_7^2 - (a_5^6 + a_12^2))x$$
$$+ a_5^4 + a_5^2 a_7 + a_2 a_7^2 + a_3 a_5 + a_2 a_3^2 + b a_{10} + b a_2 a_5^2 + b a_2^2 + b a_7 + b a_7^2 - (a_5^6 + a_12^2). \quad (21)$$

If $a_{10} \neq a^{-1} (a_3^3 + a_7^2 + a_{12}) + a_2 a_5^2 + a_2^2 + a_7^2 - (a_5^6 + a_12^2)$, then from (20) and (21) we know that $a_{14}$ is different from one value. The number of hyperelliptic curves of this kind is

$$\frac{1}{2} (q^2 - q) \cdot q \cdot (q - 1) \cdot (q - 1) = \frac{1}{2} q^3 (q - 1)^3.$$

If $a_{10} = a^{-1} (a_3^3 + a_7^2 + a_{12}) + a_2 a_5^2 + a_2^2 + a_7^2 - (a_5^6 + a_12^2)$, then from (20) and (21), we have that

$$(a_{10} + a_2 a_5^2 + a_7^2 + a_7^{-2} (a_5^6 + a_12^2))a^2 + (a_3^3 + a_7^2 + a_{12})a + a_5^4 + a_5^2 a_7 + a_2 a_7^2$$
$$= a_5^4 + a_5^2 a_7 + a_2 a_7^2 + b a_{10} + b a_2 a_5^2 + b a_2^2 + b a_7 + b a_7^2 (a_5^6 + a_12^2)$$

if and only if $a_{12} = a_3^3 + a_7^2$.

Thus, furthermore, if $a_{12} = a_3^3 + a_7^2$, then from (20) and (21) we know that $a_{14}$ is different from one value. The number of hyperelliptic curves of this kind is

$$\frac{1}{2} (q^2 - q) \cdot q \cdot 1 \cdot (q - 1) = \frac{1}{2} q^2 (q - 1)^2.$$

And if $a_{12} \neq a_3^3 + a_7^2$, then from (20) and (21) we know that $a_{14}$ is different from two values. The number of hyperelliptic curves of this kind is

$$\frac{1}{2} (q^2 - q) \cdot q \cdot (q - 1) \cdot (q - 2) = \frac{1}{2} q^2 (q - 1)^2 (q - 2).$$

Then in Case (ii) the number of hyperelliptic curves of form (16) is

$$\frac{1}{2} q^3 (q - 1)^3 + \frac{1}{2} q^2 (q - 1)^2 + \frac{1}{2} q^2 (q - 1)^2 (q - 2) = \frac{1}{2} q^2 (q - 1)^3 (q + 1).$$
Case (iii): $h(u)$ decomposes over $\mathbb{F}_q$ as the product of three polynomials of degree one. That is $u^3 + asu + a_7 = (u + a)(u + b)(u + a + b), a, b, a \in \mathbb{F}_q^*, a \neq b$. The number of this kind of $h$ is $\frac{1}{6}(q - 1)(q - 2)$. And we have $a_5 = ab + a^2 + b^2, a_7 = ab(a + b).$ And $x$ in (19) may be $a, b, a + b$. Define

\[
\begin{align*}
\alpha &= a_{10} + a_2a_5^2 + a_7^2 + a_{12}^{-2}(a_5^6 + a_{12}^2), \\
\beta &= a_{12}^3 + a_7^2 + a_{12}, \\
\gamma &= a_{12}^3 + a_7^2a_7 + a_2a_7^2,
\end{align*}
\]

thus, (19) turns into

\[
a_{14} \neq \alpha x^2 + \beta x + \gamma, \quad x = a, b, a + b. \tag{22}
\]

If $\alpha = \beta = 0$, i.e., $a_{12} = a_3^2 + a_7^2, a_{10} = a_2a_5^2 + a_7^2 + a_{12}^{-2}(a_5^6 + a_{12}^2) = a_2a_7^2$, then by (22) we know that $a_{14}$ is different from one value. The number of hyperelliptic curves of this kind is

\[
\frac{1}{6} (q - 1)(q - 2) \cdot q \cdot 1 \cdot 1 \cdot (q - 1) = \frac{1}{6} q(q - 1)^2(q - 2).
\]

If $\alpha = 0, \beta \neq 0$, then by (22) we know that $a_{14}$ is different from three values. The number of hyperelliptic curves of this kind is

\[
\frac{1}{6} (q - 1)(q - 2) \cdot q \cdot (q - 1) \cdot 1 \cdot (q - 3) = \frac{1}{6} q(q - 1)^2(q - 2)(q - 3).
\]

If $\alpha \neq 0, \beta = 0$, then by (22) we know that $a_{14}$ is different from three values. The number of hyperelliptic curves of this kind is

\[
\frac{1}{6} (q - 1)(q - 2) \cdot q \cdot 1 \cdot (q - 1) \cdot (q - 3) = \frac{1}{6} q(q - 1)^2(q - 2)(q - 3).
\]

If $\alpha \neq 0, \beta \neq 0$, then it is easy to see when $h(\frac{\beta}{\alpha}) = 0$ holds, by (22), $a_{14}$ is different from two values; when $h(\frac{\beta}{\alpha}) \neq 0$ holds, by (22), $a_{14}$ is different from three values. Let $x$ be a root of $h$, and $\frac{\beta}{\alpha} = x$ is just

\[
a_{10} = a_2a_5^2 + a_7^2 + a_{12}^{-2}(a_5^6 + a_{12}^2) + x^{-1}(a_3^3 + a_7^2 + a_{12}).
\]

Thus, if $h(\frac{\beta}{\alpha}) = 0$, then $a_{10}$ has three possibilities. The number of hyperelliptic curves of this kind is

\[
\frac{1}{6} (q - 1)(q - 2) \cdot q \cdot (q - 1) \cdot 3 \cdot (q - 2) = \frac{3}{6} q(q - 1)^2(q - 2)^2.
\]
If $h(\frac{\beta}{\gamma}) \neq 0$, then $a_{10}$ is different from four values. The number of hyperelliptic curves of this kind is

$$\frac{1}{6} (q - 1)(q - 2) \cdot q \cdot (q - 1) \cdot (q - 4) \cdot (q - 3) = \frac{1}{6} q(q - 1)^2(q - 2)(q - 3)(q - 4).$$

Thus, in Case (iii) the number of hyperelliptic curves is

$$\frac{1}{6} q(q - 1)^2(q - 2) + \frac{1}{6} q(q - 1)^2(q - 2)(q - 3) + \frac{1}{6} q(q - 1)^2(q - 2)(q - 3)$$

$$+ \frac{3}{8} q(q - 1)^2(q - 2)^2 + \frac{1}{8} q(q - 1)^2(q - 2)(q - 3)(q - 4) = \frac{1}{6} q(q - 1)^4(q - 2).$$

So the number of hyperelliptic curves of form (16) is

$$q^3(q - 1) + q^2(q - 1)^3 + \frac{1}{3} q(q^2 - 1)(q^3 - 1) + \frac{1}{2} q^2(q - 1)^3(q + 1) + \frac{1}{6} q(q - 1)^4(q - 2)$$

$$= q^5(q - 1),$$

and

$$N_1 = \frac{q^5(q - 1)}{q/2} = 2q^5 - 2q^4. \quad \Box$$

6.2. Type II: $a_1 = 0, a_3 \neq 0$

Suppose $a_1 = 0, a_3 \neq 0$. Putting

$$\gamma = (\beta^2 + a_4)/a_3,$$

$$\theta = (\beta^4 + \beta^2\gamma a_3 + \delta a_5 + \beta\gamma a_5 + \gamma a_7 + a_8)/a_3,$$

$$\epsilon = (\beta^5 + \theta^2 + \beta^2 a_2 + \beta^2 a_3 + \theta a_5 + \beta\delta a_5 + \delta a_7 + \beta a_8 + a_{10})/a_3,$$

by (15) we have $a_4 = a_8 = a_{10} = 0$. So below we can suppose $a_4 = a_8 = a_{10} = 0$. Now the Weierstrass equation turns into

$$u^2 + (a_3 u^2 + a_5 u + a_7) v = u^7 + a_2 u^6 + a_6 u^4 + a_{12} u + a_{14}, \quad a_3 \neq 0. \quad (23)$$

And (15) turns into

$$\begin{align*}
\lambda^3 a_3 &= a_3, \\
\lambda^5 a_5 &= a_5, \\
\lambda^7 a_7 &= \beta^2 a_3 + \beta a_5 + a_7, \\
\lambda^2 a_2 &= \beta + \gamma^2 + a_2, \\
\lambda^6 a_6 &= \beta^3 + \delta^2 + \beta^2 a_2 + \delta a_3 + \gamma a_5 + a_6, \\
\lambda^{12} a_{12} &= \beta^6 + \beta^2 \theta a_3 + (\epsilon + \beta \theta)a_5 + \theta a_7 + a_{12}, \\
\lambda^{14} a_{14} &= \beta^7 + \epsilon^2 + \beta^6 a_2 + \beta^2 \epsilon a_3 + \beta \epsilon a_5 + \beta^4 a_6 + \epsilon a_7 + \beta a_{12} + a_{14}.
\end{align*} \quad (24)$$
and

\[
\begin{align*}
\beta^2 + \gamma a_3 &= 0, \\
\beta^4 + (\theta + \beta^2\gamma)a_3 + (\delta + \beta\gamma)a_5 + \gamma a_7 &= 0, \\
\beta^5 + \theta^2 + \beta^3 a_2 + (\varepsilon + \beta^2\delta)a_3 + (\theta + \beta\delta)a_5 + \delta a_7 &= 0.
\end{align*}
\]  

(25)

From (25), we know that \(\gamma, \theta, \varepsilon\) are determined by \(\beta\) and \(\delta\). Thus, the group of the coordinate transformation is determined by \(x, \beta\) and \(\delta\), its order is \(q^2(q - 1)\). Below we first count the number of hyperelliptic curves of form (23).

**Proposition 6.2.** The number of hyperelliptic curves of form (23) is \(q^5(q - 1)^2\).

**Proof.** Eq. (23) represents a hyperelliptic curve if and only if there are no \((x, y) \in \mathbb{F}_q \times \mathbb{F}_q\) satisfying

\[
\begin{align*}
y^2 &= f(x), \\
h(x) &= 0, \\
yh'(x) &= f'(x),
\end{align*}
\]  

(26)

where \(h(u) = a_3u^2 + a_5u + a_7, f(u) = u^7 + a_2u^6 + a_6u^4 + a_{12}u + a_{14}\). Since \(h'(u) = a_5, f'(u) = u^6 + a_{12}\), we will distinguish two cases.

Suppose \(a_5 = 0\). \(h(x) = 0\) implies \(x^2 = a_7\), and \(f'(x) = x^6 + a_{12} = a_3 + a_{12}\). No solution of (26) is equivalent to \(a_{12} \neq a_3^3\). The number of hyperelliptic curves of this kind is \(q^4(q - 1)^2\).

Suppose \(a_5 \neq 0\). No solution of (26) is equivalent to

\[
\left( \frac{x^6 + a_{12}}{a_5} \right)^2 \neq f(x),
\]

(27)

where \(a_3x^2 + a_5x + a_7 = 0\).

An easy computation shows that (27) is just

\[
\begin{align*}
a_{14} &\neq (a_3^{-11}a_5^9 + a_3^{-7}a_5a_7^4 + a_3^{-6}a_5^6 + a_3^{-5}a_5^4a_7 + a_3^{-3}a_5^3a_7 + a_2a_5^{-5}a_5^5 + a_2a_5^{-3}a_5a_7^2
\\ &+ a_3^{-3}a_5^2a_6 + a_{12})x + a_5^{-11}a_5^8a_7 + a_3^{-7}a_5^4a_7 + a_3^{-10}a_5^6a_7^2 + a_5^{-8}a_5^2a_7^4
\\ &+ a_3^{-6}a_5^{-2}a_7^6 + a_5^{-2}a_1^2 + a_3^{-6}a_5^2a_7 + a_3^{-4}a_5a_7^3 + a_2a_5^{-5}a_5^4a_7 + a_2a_5^{-4}a_5^2a_7^2
\\ &+ a_2a_5^{-3}a_7^3 + a_3^{-3}a_5^2a_6a_7 + a_3^{-2}a_6a_7^2.
\end{align*}
\]  

(28)
Denote the coefficient of \( x \) of the right-hand side of (28) by \( a \). Let \( \tilde{h}(u) = u^2 + a_3^{-1} a_5 u + a_3^{-1} a_7 \). Obviously, \( a = 0 \) is just

\[
a_{12} = a_3^{-11} a_5^9 + a_3^{-7} a_5 a_7^4 + a_3^{-6} a_5^6 + a_3^{-5} a_5^4 a_7 + a_3^{-3} a_5^3 + a_2 a_3^{-5} a_5^5 + a_2 a_3^{-3} a_5 a_7^2 + a_3^{-3} a_5^3 a_6.
\]

Suppose \( \tilde{h} \) is irreducible over \( \mathbb{F}_q \). The number of this kind of \( \tilde{h} \) is \( \frac{1}{2} (q^2 - q) \).

If \( a \neq 0 \), then by (28) we know that \( a_{14} \) can be arbitrary. The number of hyperelliptic curves of this kind is

\[
(q - 1) \cdot \frac{1}{2} (q^2 - q) \cdot q \cdot q \cdot (q - 1) \cdot q = \frac{1}{2} q^4 (q - 1)^3.
\]

If \( a = 0 \), then by (28) we know that \( a_{14} \) is different from one value. The number of hyperelliptic curves of this kind is

\[
(q - 1) \cdot \frac{1}{2} (q^2 - q) \cdot q \cdot q \cdot 1 \cdot (q - 1) = \frac{1}{2} q^3 (q - 1)^3.
\]

Suppose \( \tilde{h} \) is reducible over \( \mathbb{F}_q \). The number of this kind of \( \tilde{h} \) is \( (q - 1) q - \frac{1}{2} (q^2 - q) = \frac{1}{2} (q^2 - q) \).

If \( a \neq 0 \), then by (28) we know that \( a_{14} \) is different from two values. The number of hyperelliptic curves of this kind is

\[
(q - 1) \cdot \frac{1}{2} (q^2 - q) \cdot q \cdot q \cdot (q - 1) \cdot (q - 2) = \frac{1}{2} q^3 (q - 1)^3 (q - 2).
\]

If \( a = 0 \), then by (28) we know that \( a_{14} \) is different from one value. The number of hyperelliptic curves of this kind is

\[
(q - 1) \cdot \frac{1}{2} (q^2 - q) \cdot q \cdot q \cdot 1 \cdot (q - 1) = \frac{1}{2} q^3 (q - 1)^3.
\]

Hence, when \( a_5 \neq 0 \) holds, the number of hyperelliptic curves of form (23) is

\[
\frac{1}{2} q^4 (q - 1)^3 + \frac{1}{2} q^3 (q - 1)^3 + \frac{1}{2} q^3 (q - 1)^3 (q - 2) + \frac{1}{2} q^3 (q - 1)^3 = q^4 (q - 1)^3.
\]

Thus, the number of hyperelliptic curves of form (23) is

\[
q^4 (q - 1)^2 + q^4 (q - 1)^3 = q^5 (q - 1)^2. \quad \square
\]
Below we will analyze the size of the stabilizer. By (24), in the stabilizer we have

\[
\begin{align*}
\begin{cases}
x^3 &= 1, \\
x^2a_5 &= a_5, \\
x_5a_7 &= \beta^2a_3 + \beta a_5 + a_7, \\
x^2a_2 &= \beta + \gamma^2 + a_2, \\
0 &= \beta^3 + \delta^2 + \beta^2a_2 + \delta a_3 + \gamma a_5, \\
0 &= \beta^6 + \beta^2\theta a_3 + (\varepsilon + \beta\theta)a_5 + \theta a_7, \\
x^2a_{14} &= \beta^7 + \varepsilon^2 + \beta^6a_2 + \beta^2\varepsilon a_3 + \beta\varepsilon a_5 + \beta^4a_6 + \varepsilon a_7 + \beta a_{12} + a_{14}. 
\end{cases}
\end{align*}
\]  

(29)

**Lemma 6.3.** The size of any stabilizer must be at least 2, i.e., \( x = 1, \beta = 0, \delta = 0, a_3 \) must be in any stabilizer.

**Proof.** When \( x = 1, \beta = 0, \delta = 0, a_3 \) hold, to see whether they are in a stabilizer, it needs to see whether (25) and (29) hold. By the first formula of (25), we have \( x = 0 \). Thus, the first five formulae of (29) all hold. By the second formula of (25), we have \( \theta a_3 = \delta a_5 \). By the third formula of (25), we have \( \varepsilon a_3 = \theta^2 + \theta a_5 + \delta a_7 \). Hence

\[
\varepsilon a_3 = \left( \frac{\delta a_5}{a_3} \right)^2 + \frac{\delta a_5}{a_3} \cdot a_5 + \delta a_7 = \delta a_7.
\]

Thus,

\[
\varepsilon a_5 + \theta a_7 = \frac{\delta a_7}{a_3} \cdot a_5 + \frac{\delta a_5}{a_3} \cdot a_7 = 0,
\]

so the sixth formula of (29) holds. And

\[
\varepsilon^2 + \varepsilon a_7 = \left( \frac{\delta a_7}{a_3} \right)^2 + \frac{\delta a_7}{a_3} \cdot a_7 = 0,
\]

so the seventh formula of (29) holds. This completes the proof. \( \square \)

**Lemma 6.4.** Suppose in the stabilizer we must have \( x = 1 \). Then if and only if \( a_5^2, \text{Tr}_{q/2}(a_2a_3^{-4}a_5^2) = 0, \) and \( a_{12} = a_3^{-6}a_5^6 + a_2a_3^{-5}a_5^4 + a_3^{-3}a_5^2 + a_2a_3^{-3}a_5a_7^2 + a_3^{-1}a_5^3 + a_3^{-7}a_5a_4^4 + a_5a_7 + a_3^{-3}a_3^3 \) hold, the size of the stabilizer is 4, otherwise the size of the stabilizer is 2.
Proof. Since \( z = 1 \), (29) turns into

\[
\begin{aligned}
0 &= \beta^2 a_3 + \beta a_5, \\
0 &= \beta + \gamma^2, \\
0 &= \beta^3 + \delta^2 + \beta^2 a_2 + \delta a_3 + \gamma a_5, \\
0 &= \beta^5 + \beta^2 a_3 + (\epsilon + \beta \theta) a_5 + \theta a_7, \\
0 &= \beta^7 + \epsilon^2 + \beta^5 a_2 + \beta^2 \epsilon a_3 + \beta \epsilon a_5 + \beta^4 a_6 + \epsilon a_7 + \beta a_{12}.
\end{aligned}
\]  

(30)

Here \( a_3 \neq 0 \). If \( a_5 = 0 \), then by the first formula of (30) we have \( \beta = 0 \), by the second formula of (30) we have \( \gamma = 0 \), by the third formula of (30) we have \( \delta = 0, a_3 \).

By Lemma 6.3, the size of the stabilizer is 2. If \( a_5 \neq 0 \), by the first formula of (30), except \( \beta = 0 \), we also have \( \beta = a_3^{-1} a_5 \). Below suppose \( \beta = a_3^{-1} a_5 \). By the first formula of (25), we have \( \gamma = \beta^2 \cdot a_3^{-1} = a_3^{-3} a_5^2 \). Again by the second formula of (30), we have \( \beta = \gamma = a_3^{-6} a_5^4 \). Hence we have \( a_3^{-1} a_5 = a_3^{-6} a_5^4 \), i.e., \( a_3^5 = a_5^3 \). Thus, if \( a_3^5 \neq a_5^3 \), then \( \beta = a_3^{-1} a_5 \) is impossible, the size of the stabilizer still is 2. Below suppose \( a_3^5 = a_5^3 \).

By the third formula of (30), we have

\[
\delta^2 + \delta a_3 = \beta^3 + \beta^2 a_2 + \gamma a_5 = (a_3^{-1} a_5)^3 + (a_3^{-1} a_5)^2 \cdot a_2 + a_3^{-3} a_5^2 \cdot a_5 = a_2 a_3^{-2} a_5^2.
\]

By Corollary 5.2, the above expression has a solution \( \delta \in \mathbb{F}_q \) if and only if

\[
\text{Tr}_{q/2} \left( \frac{a_2 a_3^{-2} a_5^2}{a_3^2} \right) = \text{Tr}_{q/2}(a_2 a_3^{-4} a_5^2) = 0.
\]

Hence if the expression \( \text{Tr}_{q/2}(a_2 a_3^{-4} a_5^2) = 0 \) does not hold, the size of the stabilizer still is 2. Below suppose \( \text{Tr}_{q/2}(a_2 a_3^{-4} a_5^2) = 0 \).

By the second formula of (25), we have

\[
\theta = a_3^{-1}(\beta^4 + \beta^2 \gamma a_3 + (\delta + \beta \gamma) a_5 + \gamma a_7) \\
= a_3^{-1}(a_3^{-1} a_5)^2 + (a_3^{-1} a_5)^2 \cdot a_3^{-3} a_5^2 \cdot a_3 + \delta a_5 + a_3^{-1} a_5 \cdot a_3^{-3} a_5^2 \cdot a_5 + a_3^{-3} a_5^2 \cdot a_7) \\
= a_5 + \delta a_3^{-1} a_5 + a_3^{-4} a_5^2 a_7.
\]

Similarly, by the third formula of (25) we have

\[
\epsilon = a_3^{-1} a_5^2 + \delta a_3^{-1} a_7 + a_3^{-4} a_5 a_7^2 + a_7.
\]

Now we consider the fourth formula of (30):

\[
\beta^6 + \beta^2 \theta a_3 + (\epsilon + \beta \theta) a_5 + \theta a_7 = \beta^6 + \epsilon a_5 + \theta a_7 + \beta^2 \theta a_3 + \beta \theta a_5 = \beta^6 + \epsilon a_5 + \theta a_7
\]
\[ \begin{align*}
\delta &:\quad \begin{array}{c}
(a_3^{-1}a_5)^6 + a_5(a_3^{-1}a_5^2 + \delta a_3^{-1}a_7 + a_3^{-4}a_5a_7^2 + a_7) \\
+ a_7(a_5 + \delta a_3^{-1}a_5 + a_3^{-4}a_5^2a_7) = 0,
\end{array}
\end{align*} \]

hence the fourth formula of (30) holds. If the fifth formula of (30) holds, as \( \beta = a_3^{-1}a_5 \neq 0 \), then the fifth formula of (30) is

\[ a_{12} = \beta^6 + \beta^5a_2 + \beta^3a_6 + \beta a_2a_3 + a_2a_3^{-3}a_5a_7^2 + a_3^{-1}a_5^3 + a_3^{-7}a_5a_7^4 + a_5a_7 + a_3^{-3}a_7^3. \]

Thus, if the above expression holds, the size of the stabilizer is 4, otherwise the size of the stabilizer still is 2. This completes the proof of the lemma. \( \square \)

**Proposition 6.5.** Suppose \( m \) is odd. Let \( N_2 \) denote the number of isomorphism classes of hyperelliptic curves of form (23), then \( N_2 = q(q-1)(2q^2 + 1) \).

**Proof.** For \( m \) is odd, we have \( 3 \mid (q - 1) \). Then by the first formula of (29), in the stabilizer we must have \( x = 1 \). Thus by Lemma 6.4, when \( a_5 = a_5^3 \), \( \text{Tr}_{q/2}(a_2a_3^{-4}a_5^2) = 0 \), and \( a_{12} = a_3^{-6}a_5^6 + a_2a_3^{-5}a_5^5 + a_3^{-3}a_5^3a_6 + a_2a_3^{-3}a_5a_7^2 + a_3^{-1}a_5^3 + a_3^{-7}a_5a_7^4 + a_5a_7 + a_3^{-3}a_7^3 \) hold, the size of the stabilizer is 4 (otherwise the size of the stabilizer is 2).

To compute \( N_2 \), we need to count the number of hyperelliptic curves of form (23) when these conditions hold. It is easy to see that the coefficient of \( x \) in (28) is 0. Hence the number of hyperelliptic curves of this kind is

\[ (q - 1) \cdot 1 \cdot \frac{q}{2} \cdot q \cdot 1 \cdot (q - 1) = \frac{1}{2}q^3(q - 1)^2. \]

Thus by Proposition 6.2 we have

\[ N_2 = \frac{1}{2}q^3(q - 1)^2 + \frac{q^5(q - 1)^2 - \frac{1}{2}q^3(q - 1)^2}{q^2(q - 1)/2} = q(q - 1)(2q^2 + 1). \quad \square \]

**Proposition 6.6.** Suppose \( m \) is even. Let \( N_2 \) denote the number of isomorphism classes of hyperelliptic curves of form (23), then \( N_2 = 2q^4 - 2q^3 + q^2 - 3q - 4 \).

**Proof.** For \( m \) is even, we have \( 3 \mid (q - 1) \). Combining with \( x^2 = 1 \), so in the stabilizer we must have \( x = 1 \). Then by Lemma 6.4, when \( a_3 = a_3^2 \), \( \text{Tr}_{q/2}(a_2a_3^{-4}a_5^2) = 0 \), and \( a_{12} = a_3^{-6}a_5^6 + a_2a_3^{-5}a_5^5 + a_3^{-3}a_5^3a_6 + a_2a_3^{-3}a_5a_7^2 + a_3^{-1}a_5^3 + a_3^{-7}a_5a_7^4 + a_5a_7 + a_3^{-3}a_7^3 \) hold, the size of the stabilizer is 4 (otherwise the size of the stabilizer is 2). And the number of
hyperelliptic curves of this kind is
\[
\frac{q - 1}{3} \cdot 3 \cdot \frac{q}{2} \cdot q \cdot 1 \cdot (q - 1) = \frac{1}{2} q^3 (q - 1)^2.
\]
Thus, when \( a_5 \neq 0 \) holds, the number of isomorphism classes of hyperelliptic curves of form (23) is
\[
\frac{1}{2} q^3 (q - 1)^2 + \frac{q^4(q - 1)^3 - \frac{1}{2} q^3(q - 1)^2}{q^2(q - 1)/2} = q(q - 1)(2q^2 - 2q + 1).
\]
If \( a_5 = 0 \), then (23) turns into
\[
v^2 + (a_3 u^2 + a_7)v = u^7 + a_2 u^6 + a_6 u^4 + a_{12} u + a_{14}, \quad a_3 \neq 0.
\] (31)
Eqs. (24) and (25) turn into
\[
\left\{
\begin{array}{l}
x^3 a_3 = a_3, \\
x^7 a_7 = \beta^2 a_3 + a_7, \\
x^2 a_2 = \beta + \gamma^2 + a_2, \\
x^6 a_6 = \beta^3 + \delta^2 + \beta^2 a_2 + \delta a_3 + a_6, \\
x^{12} a_{12} = \beta^6 + \beta^2 \theta a_3 + \theta a_7 + a_{12}, \\
x^{14} a_{14} = \beta^7 + \epsilon^2 + \beta^6 a_2 + \beta^2 \epsilon a_3 + \beta^4 a_6 + \epsilon a_7 + \beta a_{12} + a_{14}
\end{array}
\right.
\] (32)
and
\[
\left\{
\begin{array}{l}
\beta^2 + \gamma a_3 = 0, \\
\beta^4 + (\theta + \beta^2 \gamma) a_3 + \gamma a_7 = 0, \\
\beta^5 + \theta^2 + \beta^4 a_2 + (\epsilon + \beta^2 \delta) a_3 + \delta a_7 = 0.
\end{array}
\right.
\] (33)
Putting \( \beta^2 = \frac{a_7}{a_3} \), we have \( a_7 = 0 \). So below suppose \( a_7 = 0 \). Eq. (31) turns into
\[
v^2 + a_3 u^2 v = u^7 + a_2 u^6 + a_6 u^4 + a_{12} u + a_{14}, \quad a_3 \neq 0.
\] (34)
Eqs. (32) and (33) turn into (necessarily \( \beta = \gamma = \theta = \epsilon = 0 \), (33) automatically holds)
\[
\left\{
\begin{array}{l}
x^3 a_3 = a_3, \\
x^2 a_2 = a_2, \\
x^6 a_6 = \delta^2 + \delta a_3 + a_6, \\
x^{12} a_{12} = a_{12}, \\
x^{14} a_{14} = a_{14}.
\end{array}
\right.
\] (35)
Thus, the group of the coordinate transformation is determined by $z$ and $\delta$, its order is $q(q - 1)$. From the proof of Proposition 6.2 we know that if and only if $a_{12} \neq 0$, (34) represents a hyperelliptic curve. So the number of hyperelliptic curves of form (34) is $q^3(q - 1)^2$. And in the stabilizer, by (35) we have

$$\left\{ \begin{array}{l} x^3 = 1, \\
x^2a_2 = a_2, \\
0 = \delta^2 + \delta a_3, \\
x^{14}a_{14} = a_{14}. \end{array} \right. \quad (36)$$

From (36) we know when $a_2 = a_{14} = 0$, the size of the stabilizer is 6, otherwise the size of the stabilizer is 2. Hence the number of isomorphism classes of hyperelliptic curves of form (34) is

$$\frac{q(q - 1)^2}{q(q - 1)/6} + \frac{q^3(q - 1)^2 - q(q - 1)^2}{q(q - 1)/2} = 2(q - 1)(q^2 + 2).$$

Therefore,

$$N_2 = q(q - 1)(2q^2 - 2q + 1) + 2(q - 1)(q^2 + 2) = 2q^4 - 2q^3 + q^2 + 3q - 4. \quad \square$$

6.3. Type III: $a_1 = a_3 = 0, a_5 \neq 0$

Suppose $a_1 = a_3 = 0, a_5 \neq 0$. Putting

$$\beta = a_7/a_5,$$
$$\gamma^2 = \beta + a_2,$$
$$\delta^2 = \beta^3 + \beta^2a_2 + \beta a_4 + \gamma a_5 + a_6,$$
$$\varepsilon = (\beta^6 + \beta^4a_4 + \beta^2a_5 + \beta a_7 + \beta^2a_8 + a_{12})/a_5,$$

by (15), we have $a_7 = a_2 = a_6 = a_{12} = 0$. So we can suppose $a_7 = a_2 = a_6 = a_{12} = 0$. Now the Weierstrass equation turns into

$$v^2 + a_5uv = u^7 + a_4u^5 + a_8u^3 + a_{10}u^2 + a_{14}, \quad a_5 \neq 0. \quad (37)$$

And (15) turns into (necessarily $\beta = \gamma = \delta = \varepsilon = 0$)

$$\left\{ \begin{array}{l} x^5a_5 = a_5, \\
x^4a_4 = a_4, \\
x^8a_8 = a_8, \\
x^{10}a_{10} = \theta^2 + \theta a_5 + a_{10}, \\
x^{14}a_{14} = a_{14}. \end{array} \right. \quad (38)$$
Hence the group of the coordinate transformation is determined by \( x \) and \( \theta \), its order is \( q(q - 1) \). Obviously, if and only if \( a_{14} \neq 0 \), (37) represents a hyperelliptic curve. And the size of the stabilizer is 2. So the number of isomorphism classes of hyperelliptic curves of form (37) is

\[
\frac{q^3(q - 1)^2}{q(q - 1)/2} = 2q^2(q - 1).
\]

Therefore we get the following.

**Proposition 6.7.** Let \( N_3 \) denote the number of isomorphism classes of hyperelliptic curves of form (37), then we have \( N_3 = 2q^2(q - 1) \).

6.4. Type IV: \( a_1 = a_3 = a_5 = 0, a_7 \neq 0 \)

Suppose \( a_1 = a_3 = a_5 = 0, a_7 \neq 0 \). Putting

\[
\begin{align*}
\beta^2 &= a_4, \\
\gamma^2 &= \beta + a_2, \\
\delta^2 &= \beta^3 + \beta^2a_2 + \beta a_4 + a_6, \\
\theta^2 &= \beta^5 + \beta^4a_2 + \delta a_7 + \beta a_8 + a_{10},
\end{align*}
\]

by (15), we have \( \bar{a}_4 = \bar{a}_2 = \bar{a}_6 = \bar{a}_{10} = 0 \). So we can suppose \( a_4 = a_2 = a_6 = a_{10} = 0 \). Now the Weierstrass equation turns into

\[
v^2 + a_7v = u^7 + a_8u^3 + a_{12}u + a_{14}, \quad a_7 \neq 0.
\]

And (15) turns into (necessarily \( \beta = \gamma = \delta = \theta = 0 \))

\[
\begin{align*}
\alpha^7\bar{a}_7 &= a_7, \\
\alpha^8\bar{a}_8 &= a_8, \\
\alpha^{12}\bar{a}_{12} &= a_{12}, \\
\alpha^{14}\bar{a}_{14} &= \epsilon^2 + \epsilon a_7 + a_{14}.
\end{align*}
\]

Thus, the group of the coordinate transformation is determined by \( x \) and \( \epsilon \), its order is \( q(q - 1) \).

**Proposition 6.8.** Let \( N_4 \) denote the number of isomorphism classes of hyperelliptic curves of form (39), then we have

\[
N_4 = \begin{cases} 
2q^2 + 12, & 3 \mid m, \\
2q^2, & 3 \nmid m. 
\end{cases}
\]
Proof. For $3 \nmid m$, we have $7 \nmid (q - 1)$. Hence in the stabilizer we must have $x = 1$, the size of the stabilizer is 2. Thus,

$$N_4 = \frac{q^3(q - 1)}{q(q - 1)/2} = 2q^2.$$  

For $3 \mid m$, we have $7 \mid (q - 1)$. If $a_8 = a_{12} = 0$, then the size of the stabilizer is 14, otherwise the size of the stabilizer is 2. Thus,

$$N_4 = \frac{q(q - 1)}{q(q - 1)/14} + \frac{q^3(q - 1) - q(q - 1)}{q(q - 1)/2} = 2q^2 + 12. \quad \Box$$

Combining above Propositions 6.1 and 6.5–6.8, we get the main result of the sixth section.

**Theorem 6.9.** Let $N$ denote the number of isomorphism classes of hyperelliptic curves of genus 3 over $\mathbb{F}_q(q = 2^n)$, then we have

<table>
<thead>
<tr>
<th>$N$</th>
<th>$3 \mid m$</th>
<th>$3 \nmid m$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 \mid m</td>
<td>$2q^5 + q^2 + 3q + 8$</td>
<td>$2q^5 + q^2 + 3q - 4$</td>
</tr>
<tr>
<td>2 \nmid m</td>
<td>$2q^5 + q^2 - q + 12$</td>
<td>$2q^5 + q^2 - q$</td>
</tr>
</tbody>
</table>

Proof. As $N = N_1 + N_2 + N_3 + N_4$, the theorem follows from Propositions 6.1 and 6.5–6.8. \quad \Box

Acknowledgements

The author would like to thank Prof. Mulan Liu for her encouragement. He wish to thank Prof. Huah Chu, Prof. Shou-Jen Hu and Prof. Ming-Chang Kang for their helpful discussions about the manuscript of this paper. He also thanks the reviewers for their helpful comments and suggestions.

References


