Isomorphism Classes of Hyperelliptic Curves of Genus 2 in Characteristic 5

L. Hernández Encinas and J. Muñoz Masqué
Instituto de Física Aplicada, CSIC
C/ Serrano 144, 28006 Madrid, Spain
E-mail: {luis, jaime}@iec.csic.es

Abstract

The reduced equations for the hyperelliptic curves of genus 2 over finite fields of 5^m elements, are given. Moreover, the number of isomorphism classes of these curves are computed. These results are relevant for the genus-2 hyperelliptic curve classification and have applications to cryptography.

Mathematics Subject Classification 2000. Primary 11G20; Secondary 11T71, 12E20, 14H45, 14H50, 94A60.

Key words and phrases. Hyperelliptic curves on finite fields, discriminant, cryptography.

Acknowledgement. Supported by Ministerio de Ciencia y Tecnología (Spain) under grant TIC2001–0586.

1 Introduction

The group of points of the Jacobian of a hyperelliptic curve has been proposed by N. Koblitz in [5]. The cases of genera $g \geq 5$ have been proved to be insecure by Adleman, DeMarrais and Huang ([1]) and Gaudry ([3]). The cases $g = 2$ and $g = 3$ still remain unbroken, as the best algorithm known takes $O(\sqrt{n})$ steps, n being the largest prime divisor of the order of the Jacobian.

In [4], the number of isomorphic classes of genus-2 hyperelliptic curves in characteristic $p \neq 2, 5$ has been obtained. In [2], some (upper and lower) bounds have been obtained for the number of isomorphic classes of genus-2 hyperelliptic curves in characteristic $p = 2$.

In the present paper we obtain the exact number of such classes in characteristic $p = 5$. It is worth mentioning the simplicity of the reduced equations in this case, which probably facilitate the use of such characteristic in applications. In any case, we think the results below are also interesting in the classification problem.

2 Preliminaries

We shall denote by $|X|$ the cardinal of a finite set X. Let $\mathbb{F}$ be a finite field. The discriminant of a polynomial $f \in \mathbb{F}[x]$ is designed by $D(f)$; *i.e.*, $D(f) = \text{resultant}(f, f')$, where f' is the derivative of f.

As is well known (*e.g.*, see [6]), every hyperelliptic curve H of genus $g = 2$ defined over $\mathbb{F}$ can be given by a Weierstrass equation

$$H\colon v^2 + h(u)\,v = f(u)\,, \tag{1}$$

where $h(u)$ is a polynomial of degree $\leq g = 2$, and $f(u)$ is a monic polynomial of degree $2g + 1 = 5$, *i.e.*,

$$h(u) = a_1u^2 + a_3u + a_5, \quad f(u) = u^5 + a_2u^4 + a_4u^3 + a_6u^2 + a_8u + a_{10}, \tag{2}$$

with all $a_i \in \mathbb{F}$.

It is easily checked that H has a unique point O at infinity. Equation (1) defining a hyperelliptic curve H of genus 2 is unique up to a change of coordinates of the form ([8, Proposition 1.2]):

$$(u, v) \mapsto \left(\alpha^2u + \beta, \alpha^5v + \alpha^4\gamma u^2 + \alpha^2\delta u + \varepsilon\right), \tag{3}$$

where $\alpha \in \mathbb{F}^*$ and $\beta, \gamma, \delta, \varepsilon \in \mathbb{F}$.

We denote the set of all hyperelliptic curves of genus g over $\mathbb{F}$ by $\mathfrak{H}_g$ and the set of their Weierstrass equations by $\mathfrak{W}_g$.

Let $\mathbb{F}_q \subset \mathbb{F}_{q^m}$ be a field extension. We recall ([7, 2.22]) that the trace of an element $\alpha \in \mathbb{F}_{q^m}$ over $\mathbb{F}_q$ is defined by

$$\text{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{m-1}}.$$

Set $\mathbb{F}^* = \mathbb{F} - \{0\}$ and we denote the algebraic closure of $\mathbb{F}$ by $\overline{\mathbb{F}}$. For each positive integer k, we set $\mathbb{F}^{(k)} = \{\alpha^k : \alpha \in \mathbb{F}\}$.

3 Char($\mathbb{F}$) = 5

In this section we assume $\mathbb{F} = \mathbb{F}_{5^m}$, $m \geq 1$. We write $\text{Tr}(\alpha)$ instead of $\text{Tr}_{\mathbb{F}_5}^{\mathbb{F}_{5^m}}(\alpha)$.

By carrying out the change of coordinates (3) in (1) and computing the values for the new coefficients $\overline{a}_i$, we obtain

$$\left\{\begin{aligned}
\alpha\overline{a}_1 &= a_1 + 2\gamma \\
\alpha^3\overline{a}_3 &= a_3 + 2\beta a_1 + 2\delta \\
\alpha^5\overline{a}_5 &= a_5 + \beta a_3 + \beta^2 a_1 + 2\varepsilon \\
\alpha^2\overline{a}_2 &= a_2 + 4\gamma a_1 + 4\gamma^2 \\
\alpha^4\overline{a}_4 &= a_4 + 4\gamma a_3 + 4\beta a_2 + (3\beta\gamma + 4\delta)a_1 + 3\gamma\delta \\
\alpha^6\overline{a}_6 &= a_6 + 4\gamma a_5 + 3\beta a_4 + 4\left(\beta\gamma + \delta\right)a_3 + \beta^2 a_2 \\
&\quad +(3\beta\delta + 4\beta^2\gamma + 4\varepsilon)a_1 + 4\delta^2 + 3\gamma\epsilon \\
\alpha^8\overline{a}_8 &= a_8 + 2\beta a_6 + 4\delta a_5 + 3\beta^2 a_4 + 4\left(\beta\delta + \varepsilon\right)a_3 \\
&\quad +4\beta^3 a_2 + (4\beta^2\delta + 3\beta\varepsilon)a_1 + 3\delta\epsilon \\
\alpha^{10}\overline{a}_{10} &= a_{10} + \beta a_8 + \beta^2 a_6 + 4\varepsilon a_5 + \beta^3 a_4 + 4\beta\varepsilon a_3 \\
&\quad +\beta^4 a_2 + 4\beta^2\varepsilon a_1 + \beta^5 + 4\varepsilon^2.
\end{aligned}\right. \tag{4}$$

Theorem 1 *Every hyperelliptic curve of genus 2 over $\mathbb{F}$ can be represented by one and only one of the following equations*

$$H_1\colon v^2 = u^5 + a_2u^4 + a_6u^2 + a_8u + a_{10}, \quad a_2 \in \mathbb{F}^* \tag{5}$$

$$H_2\colon v^2 = u^5 + a_4u^3 + a_8u + a_{10}, \quad a_4 \in \mathbb{F}^* \tag{6}$$

$$H_3\colon v^2 = u^5 + a_6u^2 + a_{10}, \quad a_6 \in \mathbb{F}^* \tag{7}$$

$$H_4\colon v^2 = u^5 + a_8u + a_{10}, \quad a_8 \in \mathbb{F}^*. \tag{8}$$

Proof. By using the formulas in (4) it is readily checked that every hyperelliptic curve of genus 2 can be represented by an equation (1) such that $h(u) = 0$; *i.e.*,

$$v^2 = u^5 + a_2u^4 + a_4u^3 + a_6u^2 + a_8u + a_{10}. \tag{9}$$

Moreover, as a simple computations shows, the only admissible changes of variables (3) transforming the equation (9) into another of the same form, are

$$(u, v) \mapsto \left(\alpha^2u + \beta, \alpha^5v\right), \quad \alpha \in \mathbb{F}^*, \beta \in \mathbb{F}, \tag{10}$$

that is, $\gamma, \delta, \varepsilon$ should vanish. Hence, the formulas (4) yield

$$\alpha^2\overline{a}_2 = a_2 \tag{11}$$

$$\alpha^4\overline{a}_4 = a_4 + 4\beta a_2 \tag{12}$$

$$\alpha^6\overline{a}_6 = a_6 + 3\beta a_4 + \beta^2a_2 \tag{13}$$

$$\alpha^8\overline{a}_8 = a_8 + 2\beta a_6 + 3\beta^2a_4 + 4\beta^3a_2 \tag{14}$$

$$\alpha^{10}\overline{a}_{10} = a_{10} + \beta a_8 + \beta^2a_6 + \beta^3a_4 + \beta^4a_2 + \beta^5. \tag{15}$$

(i) If $a_2 \neq 0$, taking $\beta = a_4/a_2$ in (12) we obtain $\overline{a}_4 = 0$. Hence, the equation (9) is reduced to

$$H_1\colon v^2 = u^5 + \overline{a}_2u^4 + \overline{a}_6u^2 + \overline{a}_8u + \overline{a}_{10}$$

by means of the change of variables

$$(u, v) \mapsto \left(\alpha^2u + \frac{a_4}{a_2}, \alpha^5v\right).$$

(ii) If $a_2 = 0$ and $a_4 \neq 0$, by taking $\beta = a_6/(2a_4)$ in (13) we have $\overline{a}_6 = 0$. Hence, the equation (9) is reduced to

$$H_2\colon v^2 = u^5 + \overline{a}_4u^3 + \overline{a}_8u + \overline{a}_{10}$$

by means of the change of variables

$$(u, v) \mapsto \left(\alpha^2u + \frac{a_6}{2a_4}, \alpha^5v\right).$$

(iii) If $a_2 = a_4 = 0$ and $a_6 \neq 0$, by taking $\beta = a_8/(3a_6)$ in (14) we obtain $\overline{a}_8 = 0$. Then, the equation (9) is reduced to

$$H_3\colon v^2 = u^5 + \overline{a}_6 u^2 + \overline{a}_{10}$$

by means of the change of variables

$$(u, v) \mapsto \left(\alpha^2 u + \frac{a_8}{3a_6}, \alpha^5 v\right).$$

(iv) Finally, if $a_2 = a_4 = a_6 = 0$ and $a_8 \neq 0$, then the equation (9) is reduced to

$$H_4\colon v^2 = u^5 + \overline{a}_8 u + \overline{a}_{10}.$$

■

3.1 Automorphism groups

Next, we compute the automorphism group of each hyperelliptic curve of genus 2. Let $\mathcal{H}_i$, $i = 1, \ldots, 4$, be the set of non-singular equations of the form (5)–(8), respectively. We set $\mathcal{H}_2 = \mathcal{H}_{21} \cup \mathcal{H}_{22}$ and $\mathcal{H}_4 = \mathcal{H}_{411} \cup \mathcal{H}_{412} \cup \mathcal{H}_{4211} \cup \mathcal{H}_{4212} \cup \mathcal{H}_{4221} \cup \mathcal{H}_{4222}$ with

$$\begin{aligned}
\mathcal{H}_{21} &= \{H_2 \in \mathcal{H}_2 : a_{10} = 0\} \\
\mathcal{H}_{22} &= \{H_2 \in \mathcal{H}_2 : a_{10} \neq 0\} \\
\mathcal{H}_{411} &= \{H_4 \in \mathcal{H}_4 : -a_8 \notin (\mathbb{F}^*)^4, m\,\text{even}\} \\
\mathcal{H}_{412} &= \{H_4 \in \mathcal{H}_4 : -a_8 \notin (\mathbb{F}^*)^4, m\,\text{odd}\} \\
\mathcal{H}_{4211} &= \{H_4 \in \mathcal{H}_4 : -a_8 \in (\mathbb{F}^*)^4, \operatorname{Tr}\left(a_{10}/\beta_0^5\right) = 0, m \text{ even}\} \\
\mathcal{H}_{4212} &= \{H_4 \in \mathcal{H}_4 : -a_8 \in (\mathbb{F}^*)^4, \operatorname{Tr}\left(a_{10}/\beta_0^5\right) \neq 0, m \text{ even}\} \\
\mathcal{H}_{4221} &= \{H_4 \in \mathcal{H}_4 : -a_8 \in (\mathbb{F}^*)^4, \operatorname{Tr}\left(a_{10}/\beta_0^5\right) = 0, m \text{ odd}\} \\
\mathcal{H}_{4222} &= \{H_4 \in \mathcal{H}_4 : -a_8 \in (\mathbb{F}^*)^4, \operatorname{Tr}\left(a_{10}/\beta_0^5\right) \neq 0, m \text{ odd}\},
\end{aligned}$$

where $\beta_0 \in \mathbb{F}^*$ is an element such that $\beta_0^4 = -a_8$.

We denote by G_i the group of changes of the form (10) transforming $\mathcal{H}_i$ into itself. According to Theorem 1, we have

$$\begin{aligned}
G_1 = G_2 = G_3 &= \{(u, v) \mapsto (\alpha^2 u, \alpha^5 v) : \alpha \in \mathbb{F}^*\} \\
G_4 &= \{(u, v) \mapsto (\alpha^2 u + \beta, \alpha^5 v) : \alpha \in \mathbb{F}^*, \beta \in \mathbb{F}\}.
\end{aligned}$$

Hence $|G_1| = |G_2| = |G_3| = q - 1$ and $|G_4| = q(q - 1)$.

Theorem 2 *Let A_i be the group of automorphisms of an arbitrary curve in each of the classes $\mathcal{H}_i$, with $i = 1, 21, 22, 3, 411, 412, 4211, 4212, 4221, 4222$. We* *have*

$$\begin{aligned} &|A_1| = 2 \\ &|A_{21}| = 4, \quad |A_{22}| = 2 \\ &|A_3| = 2 \\ &|A_{411}| = 8, \quad |A_{412}| = 4 \\ &|A_{4211}| = 40, \quad |A_{4212}| = 10, \quad |A_{4221}| = 20, \quad |A_{4222}| = 10. \end{aligned}$$

Proof. **(i)** Making the change of variables (10) in the equation H_1 (5) and imposing that the transformed curve coincides with H_1, from the expressions (11)–(15), we obtain $\beta = 0$ and $\alpha^2 = 1$. Therefore, the automorphism group for each curve of type H_1 is

$$(u, v) \mapsto (u, \alpha v), \quad \alpha^2 = 1.$$

(ii) Analogously, for the equation H_2 (6), we have $\beta = 0$, and if $a_{10} = 0$, then $\alpha^4 = 1$; if $a_{10} \neq 0$, then $\alpha^4 = \alpha^{10} = 1$, hence $\alpha^2 = 1$. Consequently, the automorphism group of the curves of type H_2 is

$$\begin{cases} (u, v) \mapsto (u, \alpha v), & \alpha^4 = 1 \quad \text{if } a_{10} = 0 \\ (u, v) \mapsto (u, \alpha v), & \alpha^2 = 1 \quad \text{if } a_{10} \neq 0. \end{cases}$$

(iii) In this case (7), a_{10} cannot vanish as the curve is assumed to be non-singular, and we obtain $\beta = 0$ and $\alpha^6 = \alpha^{10} = 1$, hence $\alpha^4 = 1$ and finally, $\alpha^2 = 1$. Therefore, the automorphism group of the curves of type H_3 is

$$(u, v) \mapsto (u, \alpha v), \quad \alpha^2 = 1.$$

(iv) For the curves of type H_4 (8) we obtain

$$\begin{aligned} \alpha^8 a_8 &= a_8 \\ \alpha^{10} a_{10} &= a_{10} + \beta a_8 + \beta^5. \end{aligned}$$

Hence $\alpha^8 = 1$, and substituting it into the second equation above, we obtain

$$\beta^5 + a_8 \beta = a_{10}(\alpha^2 - 1). \tag{16}$$

We distinguish several cases:
(a) If $-a_8 \notin (\mathbb{F}^*)^4$, then the map $x \mapsto x^5 + a_8 x$ is bijective; hence the equation (16) has a unique solution, say β_α, and the automorphism group is

$$(u, v) \mapsto \left(\alpha^2 u + \beta_\alpha, \alpha^5 v\right), \quad \alpha^8 = 1.$$

(b) If $-a_8 \in (\mathbb{F}^*)^4$, then there exists $\beta_0 \in \mathbb{F}^*$ such that $\beta_0^4 = -a_8$, and letting $\bar{\beta} = \beta / \beta_0$, the equation (16) becomes

$$\bar{\beta}^5 - \bar{\beta} = \frac{a_{10}(\alpha^2 - 1)}{\beta_0^5}. \tag{17}$$

Hence, according to ([9, Theorem 3.5]), we have: If $\mathrm{Tr}(a_{10}(\alpha^2-1)/\beta_0^5) \neq 0$, the equation (17) has no solution. If $\mathrm{Tr}(a_{10}(\alpha^2-1)/\beta_0^5) = 0$, the equation (17) has five distinct solutions: If $\bar{\beta}_\alpha$ is one of them, the other solutions are $\bar{\beta}_\alpha \pm 1$, $\bar{\beta}_\alpha \pm 2$. Then, we have the following subcases:

(b.1) If m is even, then the solutions to $\alpha^8 = 1$ are $\{\pm 1, \pm 2, \pm\sqrt{2} \pm 2\sqrt{2}\}$, and we have: If $\mathrm{Tr}(a_{10}/\beta_0^5) = 0$, then the automorphism group is

$$(u,v) \mapsto \left(\alpha^2 u + \beta, \alpha^5 v\right), \quad \alpha^8 = 1,\ \beta \in \{\beta_0\bar{\beta}_\alpha, \beta_0(\bar{\beta}_\alpha \pm 1), \beta_0(\bar{\beta}_\alpha \pm 2)\}.$$

If $\mathrm{Tr}(a_{10}/\beta_0^5) \neq 0$, then the automorphism group is

$$(u,v) \mapsto (u+\beta, \alpha v), \quad \alpha^2 = 1,\ \beta \in \{0, \beta_0\bar{\beta} : \bar{\beta}^4 = 1\}.$$

(b.2) If m is odd, then the only solutions to the equation $\alpha^8 = 1$ are $\{\pm 1, \pm 2\}$, and we have: If $\mathrm{Tr}(a_{10}/\beta_0^5) = 0$, then the automorphism group is

$$(u,v) \mapsto \left(\alpha^2 u + \beta, \alpha v\right), \quad \alpha^4 = 1,\ \beta \in \{\beta_0\bar{\beta}_\alpha, \beta_0(\bar{\beta}_\alpha \pm 1), \beta_0(\bar{\beta}_\alpha \pm 2)\}.$$

If $\mathrm{Tr}(a_{10}/\beta_0^5) \neq 0$, then the automorphism group is

$$(u,v) \mapsto (u+\beta, \alpha v), \quad \alpha^2 = 1,\ \beta \in \{0, \beta_0\bar{\beta} : \bar{\beta}^4 = 1\}.$$

■

3.2 Number of singular reduced equations

We use the following expression of the discriminant of a hyperelliptic curve of genus 2 over a field of characteristic 5: $\Delta(H) = \mathrm{discriminant}(f)$, where the curve H is defined by (9). Let us compute the number of singular reduced equations. To this end, we first compute the discriminant of each class of curves H_1–H_4. We have

$$\begin{aligned}
\Delta_1 = \Delta(H_1) &= 4a_{10}a_2^3a_8^3 + a_8^5 + 3a_2a_8^4a_6 + 3a_2^4a_8^4 + 4a_6^2a_2^2a_8^3 \\
&+ 4a_6^3a_2^2a_8a_{10} + 4a_6a_2^4a_{10}a_8^2 + 2a_6^2a_2^4a_{10}^2 + a_6^4a_2^3a_{10} \\
&+ a_6^3a_2^3a_8^2 + a_2^5a_{10}^3 + 3a_6^4a_8^2 + 3a_6^5a_{10} \\
\Delta_2 = \Delta(H_2) &= 2a_8^4a_4^2 + a_4^4a_8^3 + 3a_4^5a_{10}^2 + a_8^5 \\
\Delta_3 = \Delta(H_3) &= 3a_6^5a_{10} \\
\Delta_4 = \Delta(H_4) &= a_8^5.
\end{aligned} \tag{18}$$

Theorem 3 *If we consider the sets*

$$\begin{aligned}
W_1 &= \left\{(a_2, a_6, a_8, a_{10}) \in \mathbb{F}^4 : a_2 \neq 0, \Delta_1 = 0\right\} \\
W_{21} &= \left\{(a_4, a_8, 0) \in \mathbb{F}^3 : a_4 \neq 0, \Delta_2 = 0\right\} \\
W_{22} &= \left\{(a_4, a_8, a_{10}) \in \mathbb{F}^3 : a_4 \neq 0, a_{10} \neq 0, \Delta_2 = 0\right\},
\end{aligned}$$

then, we have

$$|W_1| = q^2(q-1)$$
$$|W_{21}| = |W_{22}| = q-1.$$

Proof. **(i)** Let $g(u) = u^5 + a_2u^4 + a_6u^2 + a_8u + a_{10} \in \mathbb{F}[u]$ with $a_2 \neq 0$ and $\Delta(g) = 0$. Then $g(u)$ has a multiple root $\alpha \in \overline{\mathbb{F}}$. Hence we have one of the following two factorizations of $g(u)$ in $\mathbb{F}[u]$:
(a) If $\alpha \in \mathbb{F}$, then $g(u) = (u-\alpha)^2(u^3 + (2\alpha + a_2)u^2 + (3\alpha^2 + 2\alpha a_2)u + 4\alpha^3 + 3\alpha^2 + a_6)$, $a_8 = \alpha^3 a_2 - 2\alpha a_6$, and $a_{10} = 4\alpha^5 + 3\alpha^4 a_2 + \alpha^2 a_6$.
(b) If $\alpha \notin \mathbb{F}$, then $g(u) = (u^2 + \lambda u + \mu)^2(u - \xi)$, with $(\lambda, \mu) \in (\mathbb{F}^* \times \mathbb{F})\backslash S$, where $S = \{(\lambda,\mu) \in \mathbb{F}^* \times \mathbb{F} : \lambda^2 - 4\mu \in \mathbb{F}^{(2)}\}$ (i.e., $(u^2 + \lambda u + \mu)$ is irreducible over $\mathbb{F}$), and $\xi = -(2\mu + \lambda^2)/(3\lambda)$.

Define the maps

$$\begin{cases} \varphi\colon \mathbb{F} \times \mathbb{F}^* \times \mathbb{F} \to W_1 \\ \psi\colon (\mathbb{F}^* \times \mathbb{F})\backslash S \to W_1 \end{cases}$$

given by

$$\begin{aligned} \varphi(\alpha, a_2, a_6) &= (u-\alpha)^2(u^3 + (2\alpha + a_2)u^2 + (3\alpha^2 + 2\alpha a_2)u + 4\alpha^3 + 3\alpha^2 + a_6) \\ \psi(\lambda, \mu) &= (u^2 + \lambda u + \mu)^2(u - \xi). \end{aligned}$$

As the parametrizations **(a)** and **(b)** are mutually excluding we have

$$|W_1| = |\operatorname{Im}\varphi| + |\operatorname{Im}\psi|.$$

Now, ψ is clearly injective so $|\operatorname{Im}\psi|$ is equal to the number of monic irreducible quadratics over $\mathbb{F}$ such that $\lambda \neq 0$, namely $\frac{1}{2}q(q-1) - \frac{1}{2}(q-1)$ [7, Theorem 3.25], hence $|\operatorname{Im}\psi| = \frac{1}{2}(q-1)^2$. Suppose now that $\varphi(\alpha, a_2, a_6) = \varphi(\overline{\alpha}, \overline{a}_2, \overline{a}_6)$, where $(\alpha, a_2, a_6) \neq (\overline{\alpha}, \overline{a}_2, \overline{a}_6)$. That is $g(u) = \overline{g}(u)$, where

$$\begin{aligned} g(u) &= (u-\alpha)^2(u^3 + (2\alpha + a_2)u^2 + (3\alpha^2 + 2\alpha a_2)u + 4\alpha^3 + 3\alpha^2 + a_6) \\ \overline{g}(u) &= (u-\overline{\alpha})^2(u^3 + (2\overline{\alpha} + \overline{a}_2)u^2 + (3\overline{\alpha}^2 + 2\overline{\alpha}\overline{a}_2)u + 4\overline{\alpha}^3 + 3\overline{\alpha}^2 + \overline{a}_6). \end{aligned}$$

We must have $\alpha \neq \overline{\alpha}$ since $\alpha = \overline{\alpha}$ implies

$$\begin{aligned} u^3 + (2\alpha + a_2)u^2 + (3\alpha^2 + 2\alpha a_2)u + 4\alpha^3 + 3\alpha^2 + a_6 = \\ u^3 + (2\overline{\alpha} + \overline{a}_2)u^2 + (3\overline{\alpha}^2 + 2\overline{\alpha}\overline{a}_2)u + 4\overline{\alpha}^3 + 3\overline{\alpha}^2 + \overline{a}_6. \end{aligned}$$

Then $a_2 = \overline{a}_2$ and $a_6 = \overline{a}_6$. Hence

$$g(u) = \overline{g}(u) = (u-\alpha)^2(u-\overline{\alpha})^2(u-\delta), \tag{19}$$

where

$$\begin{aligned} \delta &= -\frac{(\alpha + \overline{\alpha})^2 + 2\alpha\overline{\alpha}}{2(\alpha + \overline{\alpha})} \\ a_2 &= -2(\alpha + \overline{\alpha}) - \delta \\ a_6 &= -2\alpha\overline{\alpha}(\alpha + \overline{\alpha}) - \delta(\alpha^2 + \overline{\alpha}^2 + 4\alpha\overline{\alpha}). \end{aligned}$$

Moreover, $\alpha \neq -\overline{\alpha}$ as in other case it would be $\alpha = \overline{\alpha} = 0$. The polynomials $g(u)$ in $\operatorname{Im}\varphi$ are thus parametrized by the non-ordered pairs $(\alpha, \overline{\alpha})$ such that $\alpha \neq \pm\overline{\alpha}$. Hence, there are $(q-1) + \frac{1}{2}(q-1)(q-3)$ polynomials of the form (19) and it follows that $|\operatorname{Im}\varphi| = q^2(q-1) - \frac{1}{2}(q-1)^2$. Finally, we have $|W_1| = |\operatorname{Im}\varphi| + |\operatorname{Im}\psi| = q^2(q-1)$.

(ii) We have two cases:

(a) If $a_{10} = 0$, from (18) we obtain

$$\Delta_2 = 2a_8^4 a_4^2 + a_4^4 a_8^3 + a_8^5 = (a_4^2 + a_8)^2.$$

Then $\Delta_2 = 0$ if and only if $a_8 = -a_4^2$, hence $|W_{21}| = q-1$.

(b) If $a_{10} \neq 0$, from (18) we obtain

$$a_{10} = \pm\frac{1}{3}\frac{\sqrt{-3a_4a_8}\,a_8(a_8+a_4^2)}{a_4^3}.$$

This equation has a non-zero root if and only if there exists $\lambda \in \mathbb{F}^*$, such that $a_8 = \lambda^2/(-3a_4)$ and $\lambda^2 \neq 3a_4^3$. Moreover, $\lambda^2 - 3a_4^3 = 0$ if there exists $\mu \in \mathbb{F}^*$ such that $a_4 = \mu^2/3$ and $\lambda = \pm\mu^3/3$. Hence $|W_{22}| = q-1$. ■

3.3 Number of isomorphism classes

Theorem 4 *With the same notations as in §3.1, the number of isomorphism classes of curves of genus 2 over a field $\mathbb{F}_{5^m}$ is*

$$\begin{cases} 2q^3+4, & m \text{ even} \\ 2q^3, & m \text{ odd.} \end{cases}$$

Proof. According to the results obtained in Theorems 2 and 3, we have

$$\begin{aligned}
|\mathcal{H}_1/G_1| &= \frac{|\mathcal{H}_1|}{(G_1:A_1)} = \frac{q^2(q-1)^2}{(q-1)/2} = 2q^2(q-1)\\
|\mathcal{H}_{21}/G_2| &= \frac{|\mathcal{H}_{21}|}{(G_2:A_{21})} = \frac{(q-1)(q-2)}{(q-1)/4} = 4(q-2)\\
|\mathcal{H}_{22}/G_2| &= \frac{|\mathcal{H}_{22}|}{(G_2:A_{22})} = \frac{(q-1)^2(q-2)}{(q-1)/2} = 2(q-1)(q-2)\\
|\mathcal{H}_3/G_3| &= \frac{|\mathcal{H}_3|}{(G_3:A_3)} = \frac{(q-1)^2}{(q-1)/2} = 2(q-1)\\
|\mathcal{H}_{411}/G_4| &= \frac{|\mathcal{H}_{411}|}{(G_4:A_{411})} = \frac{3}{4}\frac{q(q-1)}{q(q-1)/8} = 6\\
|\mathcal{H}_{412}/G_4| &= \frac{|\mathcal{H}_{412}|}{(G_4:A_{412})} = \frac{3}{4}\frac{q(q-1)}{q(q-1)/4} = 3\\
|\mathcal{H}_{4211}/G_4| &= \frac{|\mathcal{H}_{4211}|}{(G_4:A_{4211})} = \frac{q(q-1)/20}{q(q-1)/40} = 2\\
|\mathcal{H}_{4212}/G_4| &= \frac{|\mathcal{H}_{4212}|}{(G_4:A_{4212})} = \frac{q(q-1)/5}{q(q-1)/10} = 2
\end{aligned}$$

$$
\begin{aligned}
|\mathcal{H}_{4221}/G_4| &= \frac{|\mathcal{H}_{4221}|}{(G_4 : A_{4221})} = \frac{q(q-1)/20}{q(q-1)/20} = 1 \\
|\mathcal{H}_{4222}/G_4| &= \frac{|\mathcal{H}_{4222}|}{(G_4 : A_{4222})} = \frac{q(q-1)/5}{q(q-1)/10} = 2.
\end{aligned}
$$

Hence,

$$
\begin{aligned}
|\mathcal{H}_1/G_1| &= 2q^2(q-1) \\
|\mathcal{H}_2/G_2| &= 2(q+1)(q-2) \\
|\mathcal{H}_3/G_3| &= 2(q-1) \\
|\mathcal{H}_4/G_4| &= \begin{cases} 10, & m \text{ even} \\ 6, & m \text{ odd}, \end{cases}
\end{aligned}
$$

thus concluding. ■

References

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

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

[3] P. Gaudry, *An algorithm for solving the discrete log problem on hyperelliptic curves*, Advances in Cryptology – Eurocrypt 2000, LNCS **1807** (2000), 19–34, Springer-Verlag, Berlin.

[4] L. Hernández Encinas, Alfred J. Menezes, and J. Muñoz Masqué, *Isomorphism classes of genus-2 hyperelliptic curves over finite fields*, Appl. Algebra Engrg. Comm. Comput., (to appear).

[5] N. Koblitz, *Hyperelliptic cryptosystems*, J. Cryptology 1 (1989), 139–150.

[6] N. Koblitz, *Algebraic aspects of cryptography*, Algorithms and Computation in Mathematics, Volume 3, Springer-Verlag, Berlin, 1998.

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

[8] P. Lockhart, *On the discriminant of a hyperelliptic curve*, Trans. Am. Math. Soc. **342**, 2 (1994), 729–752.

[9] A. Menezes (ed.), I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian, *Applications of finite fields*, Kluwer Academic Publishers, Boston, 1993.