# COUNTING HYPERELLIPTIC CURVES THAT ADMIT A KOBLITZ MODEL

CEVAHIR DEMIRKIRAN AND ENRIC NART

Universitat Autònoma de Barcelona, Departament de Matemàtiques
Edifici C, 08193 Bellaterra, Barcelona, Spain

**Corresponding author:** Enric Nart, E-mail: nart@mat.uab.cat,
Telephone Nbr. +34935811453, Fax Nbr. +34935812790

**Key words:** finite field, hyperelliptic curve, hyperelliptic cryptosystem, Koblitz model, isomorphism class, Weierstrass point, rational $n$-set.

Abstract. Let $k=\mathbb{F}_q$ be a finite field of odd characteristic. We find a closed formula for the number of $k$-isomorphism classes of pointed, and non-pointed, hyperelliptic curves of genus $g$ over $k$, admitting a Koblitz model. These numbers are expressed as a polynomial in $q$ with integer coefficients (for pointed curves) and rational coefficients (for non-pointed curves). The coefficients depend on $g$ and the set of divisors of $q-1$ and $q+1$. These formulas show that the number of hyperelliptic curves of genus $g$ suitable (in principle) of cryptographic applications is asymptotically $(1-e^{-1})2q^{2g-1}$, and not $2q^{2g-1}$ as it was believed. The curves of genus $g=2$ and $g=3$ are more resistant to the attacks to the DLP; for these values of $g$ the number of curves is respectively $(91/72)q^3+O(q^2)$ and $(3641/2880)q^5+O(q^4)$.

## Introduction

In a seminal paper Neal Koblitz introduced cryptosystems of El Gamal type based on the group of $k$-rational points of the Jacobian of a hyperelliptic curve over a finite field $k$ [10]. In order to apply Cantor's algorithm for computing the group law of the Jacobian one works with non-singular Weierstrass equations of the type:

$$y^2+h(x)y=f(x), \tag{1}$$

where $h(x)$, $f(x)$ are polynomials in $k[x]$ of degree $\deg h(x)\le g$, $\deg f(x)=2g+1$, and the polynomial $f(x)$ is monic. The projective and smooth hyperelliptic curve $C$ obtained as the normalization of the projective closure of this affine curve has always a $k$-rational Weierstrass point at infinity. We say that the equation (1) is a *Koblitz model* of the curve $C$. Conversely, any hyperelliptic curve having a $k$-rational Weierstrass point admits a Koblitz model. These models have the advantage of covering simultaneously the cases of odd and even characteristic. In this paper we deal only with the odd characteristic case, and the change of variables $y=y-h(x)/2$ allows us to suppose $h(x)=0$.

Supported by the project MTM2006-11391 from the Spanish MEC.

The paper of Koblitz had an enormous impact in the cryptographic community and it was the origin of a stream of papers addressing to fundamental problems like the acceleration of the addition algorithm in the Jacobian, the computation of the number of $k$-rational points of the Jacobian, and attacks to the discrete logarithm problem.

Some interest arose also on the problem of counting the $k$-isomorphism classes of hyperelliptic curves of a given genus, admitting a Koblitz model. For genus 2 there is a nice review in [6], refering to previous work of several authors [7, 8, 1, 2, 4]. For genus 3 we can quote [3, 9, 5]. However, all these papers count $k$-isomorphism classes of *pointed* hyperelliptic curves $(C,\infty)$; the distinguished point is always the Weierstrass point at infinity and two pointed curves $(C,\infty)$, $(C',\infty')$ are considered to be isomorphic if there is a $k$-isomorphism between $C$ and $C'$ sending $\infty$ to $\infty'$. P. Lockhart translated this isomorphism condition into a concrete equivalence relation between the Koblitz models [11, Prop.1.2] and in the quoted papers the authors count the number of classes of Koblitz models under this equivalence relation.

In this paper we use another method to find for all $g>1$ a closed formula for the isomorphism classes of pointed hyperelliptic curves of genus $g$ over finite fields of odd characteristic (Theorem 3.2). For $g$ large the number of pointed curves is asymptotically $2q^{2g-1}$ (Corollary 3.3).

Also, we solve the problem of counting the $k$-isomorphism classes of hyperelliptic curves of a given genus, admitting a Koblitz model. We give a closed formula for this number of isomorphism classes in Theorem 4.1. The dominant term of the formula is

$$\left(1-\frac{1}{2!}+\frac{1}{3!}-\cdots-\frac{1}{(2g+2)!}\right)2q^{2g-1},$$

so that for $g$ large the number of curves is asymptotically $(1-e^{-1})2q^{2g-1}$ (Corollary 4.2). This number of isomorphism classes provides the real size of the bunch of curves suitable of cryptographic applications. For instance if $k$ is the field of $q$ elements with $q\equiv 1 \pmod 3$, $q>7$, the following two genus-2 curves are $k$-isomorphic

$$y^2=x(x^2-1)(x-2)(x-3/2),\qquad y^2=x(x^2-1)(x-1/2)(x-2/3),$$

through the mapping $(x,y)\mapsto(1/x,y/(\sqrt{-3}x^3))$; thus, from the point of view of cryptographic applications they are identical. Nevertheless, they are not isomorphic as pointed curves. In fact, any $k$-isomorphism between the two curves preserving the point at infinity will act as $x\mapsto ax+b$ at the level of $x$-coordinates, with $a\in k^*$, $b\in k$; this map has to preserve the sets of $x$-coordinates of Weierstrass points of both curves and it is easy to check that there is no transformation of this type sending $\{0,1,-1,2,3/2\}$ to $\{0,1,-1,1/2,2/3\}$. Thus, in the computation of isomorphism classes of pointed curves these curves count as two different curves.

To obtain our results we use a general technique for enumerating $\mathrm{PGL}_2(k)$-orbits of rational $n$-sets of $\mathbb{P}^1$ that was developed in [12] and extended to arbitrary dimension in [14]. This technique was used in [15] to obtain a formula for the total number of $k$-isomorphism classes of hyperelliptic curves. In section 1 we obtain some results on the enumeration of rational $n$-sets of algebraic varieties; the main result is Theorem 1.3 where, for a given automorphism $\gamma$ of $\mathbb{P}^1$, we compute the number of rational $n$-sets of $\mathbb{P}^1$ that are fixed by $\gamma$ and contain at least one rational point. In section 2 we recall some results concerning the classification of hyperelliptic curves up to $k$-isomorphism. In section 3 we count pointed hyperelliptic curves by analyzing the action of the affine group on rational $(2g+1)$-sets of the affine line. In section 4 we count hyperelliptic curves admitting a rational Weierstrass point by analyzing the action of the projective group on rational $(2g+2)$-sets of the projective line, containing at least one rational point.

**Notations.** We fix once and for all a finite field $k = \mathbb{F}_q$ of odd characteristic $p$ and an algebraic closure $\overline{k}$ of $k$. We denote by $\sigma \in \mathrm{Gal}(\overline{k}/k)$ the Frobenius automorphism, $\sigma(x) = x^q$. Also, $k_2$ will denote the unique quadratic extension of $k$ in $\overline{k}$ and $\varphi$ denotes Euler's totient function.

## 1. Rational $n$-sets of algebraic varieties

Let $V$ be an algebraic variety defined over $k$. A *rational $n$-set of $V$* is by definition a $k$-rational point of the variety $\binom{V}{n}$ of $n$-sets of $V$. Thus, a rational $n$-set $S \in \binom{V}{n}(k)$ is just an unordered family $S = \{t_1, \dots, t_n\}$ of $n$ different points of $V(\overline{k})$, which is globally invariant under the Galois action: $S = S^\sigma$.

For any subset $Z \subseteq V(k)$ of $k$-rational points of $V$ we denote

$$\binom{V}{n}_Z := \left\{ S \in \binom{V}{n}(k) \;\middle|\; S \cap Z = \emptyset \right\}.$$

$$\binom{V}{n}^Z := \left\{ S \in \binom{V}{n}(k) \;\middle|\; S \cap Z \neq \emptyset \right\}.$$

For instance, for $Z = V(k)$ we obtain in the last case the set of rational $n$-sets of $V$ containing at least one $k$-rational point. In the cases $Z = V(k)$ and $Z = \{P\}$ we use a special notation

$$\binom{V}{n}^{\mathrm{rat}} := \binom{V}{n}^{V(k)}, \qquad \binom{V}{n}^{P} := \binom{V}{n}^{\{P\}}.$$

For any pair $r$, $n$ of non-negative integers we denote:

$$a_V(r,n) := \left| \binom{V}{n}_Z \right|, \quad b_V(r,n) := \left| \binom{V}{n}^Z \right|,$$

where $Z$ is any subset of $V(k)$ with $|Z| = r$. Also, we introduce a particular notation for the extreme cases:

$$a_V(n) := a_V(0,n) = \left| \binom{V}{n}(k) \right|, \qquad b_V(n) := b_V(|V(k)|, n) = \left| \binom{V}{n}^{\mathrm{rat}} \right|.$$

Hence, $a_V(n)$ counts the total number of rational $n$-sets of $V$ whereas $b_V(n)$ counts the number of rational $n$-sets of $V$ that contain at least one rational point.

Since $\binom{V}{n}^Z$ and $\binom{V}{n}_Z$ are complementary subsets of $\binom{V}{n}(k)$ we have, for all $r,\,n\ge 0$:

$$a_V(r,n)+b_V(r,n)=a_V(n). \tag{2}$$

It is easy to compute $a_V(r,n)$ in terms of the function $a_V$:

**Lemma 1.1.** *For any algebraic variety $V$ defined over $k$:*

$$a_V(r,n)=\sum_{i=0}^{n}(-1)^i\left(\!\binom{r}{i}\!\right)a_V(n-i).$$

*Proof.* We proceed by induction on $r$. Let $Z=\{t\}$ for some $t\in V(k)$. Distributing the rational $n$-sets of $V$ into two families according to the fact that they contain $t$ or not we see that

$$a_V(n)=a_V(1,n)+a_V(1,n-1).$$

By Moebius inversion we get

$$a_V(1,n)=\sum_{i=0}^{n}(-1)^i a_V(n-i), \tag{3}$$

and the statement of the lemma is proven for $r=1$.

Suppose that the claim has been checked for all varieties $V$ and all subsets $Z\subseteq V(k)$ with $|Z|\le r-1$:

$$a_V(r-1,n)=\sum_{i=0}^{n}(-1)^i\left(\!\binom{r-1}{i}\!\right)a_V(n-i).$$

By (3) we have

$$a_V(r,n)=\sum_{i=0}^{n}(-1)^i a_V(r-1,n-i),$$

and using the two formulas we get

$$a_V(r,n)=\sum_{i=0}^{n}(-1)^i\left(\left(\!\binom{r-1}{0}\!\right)+\cdots+\left(\!\binom{r-1}{i}\!\right)\right)a_V(n-i)=$$

$$=\sum_{i=0}^{n}(-1)^i\left(\!\binom{r}{i}\!\right)a_V(n-i).$$

□

By (2) we get immediately a computation of $b_V(r,n)$:

**Corollary 1.2.** *For any algebraic variety $V$ defined over $k$:*

$$b_V(r,n)=\sum_{i=1}^{n}(-1)^{i+1}\left(\!\binom{r}{i}\!\right)a_V(n-i).$$

We prove now a result that will be crucial in the enumeration of $\mathrm{PGL}_2(k)$-orbits of rational $n$-sets of $\mathbb{P}^1$. The projective action of $\mathrm{PGL}_2(k)$ on $\mathbb{P}^1(\overline{k})$ induces a natural action of $\mathrm{PGL}_2(k)$ on the set of rational $n$-sets of $\mathbb{P}^1$.

For any $\gamma \in \mathrm{PGL}_2(k)$ we denote by $\mathrm{Fix}_\gamma$ the set of fixed points of $\gamma$ in $\mathbb{P}^1(\overline{k})$. More generally, if $X$ is a set admitting an action of $\gamma$ we denote by $\mathrm{Fix}_\gamma X$ the subset of fixed points of $\gamma$ in $X$.

**Theorem 1.3.** *Let $\gamma$ be an element of $\mathrm{PGL}_2(k)$, $\gamma \neq 1$, and let $m$ be the order of $\gamma$. Let $V$ be the open subvariety $\mathbb{P}^1 \setminus \mathrm{Fix}_\gamma$ of $\mathbb{P}^1$. Then, for any positive integer $n$*

$$\left|\mathrm{Fix}_\gamma \binom{V}{n}(k)\right| = a_V\left(n/m\right),$$

$$\left|\mathrm{Fix}_\gamma \binom{V}{n}^{\mathrm{rat}}\right| = b_V\left(|V(k)|/m, n/m\right),$$

*with the convention that $a_V(x) = 0 = b_V(r,x)$ if $x$ is not a positive integer.*

*Proof.* Let $\mathbb{P}^1/\gamma$ be the quotient variety of $\mathbb{P}^1$ under the action of the cyclic group generated by $\gamma$. The curve $\mathbb{P}^1/\gamma$ is $k$-isomorphic to $\mathbb{P}^1$ because it is normal and birrationally equivalent to $\mathbb{P}^1$ (by Lüroth's theorem). Also, the Zariski closed set $(\mathbb{P}^1/\gamma) \setminus (V/\gamma)$ is isomorphic to $\mathrm{Fix}_\gamma$ as a Galois set; therefore, $V/\gamma$ is $k$-isomorphic to $V$ too and $a_{V/\gamma}(n) = a_V(n)$, $b_{V/\gamma}(r,n) = b_V(r,n)$, for all $r$, $n$.

Consider the canonical projection

$$\pi\colon V \longrightarrow V/\gamma.$$

For any $t \in V(\overline{k})$ the $\gamma$-orbit $O_\gamma(t) = \{t, \gamma(t), \dots, \gamma^{m-1}(t)\}$ has cardinality $m$ (and not a proper divisor of $m$) [12, Lem.2.3]. Thus, if an $n$-set of $V$ is $\gamma$-invariant then necessarily $n$ is a multiple of $m$. On the other hand, the mapping $\pi$ establishes a 1-1 correspondence between $\gamma$-invariant $n$-rational sets of $V$ and rational $n/m$-sets of $V/\gamma$. In particular,

$$\left|\mathrm{Fix}_\gamma \binom{V}{n}(k)\right| = a_{V/\gamma}\left(n/m\right) = a_V\left(n/m\right).$$

The $\gamma$-orbits $O := O_\gamma(t)$ such that $O = O^\sigma$ are in 1-1 correspondence with the set of $k$-rational points of $V/\gamma$. Exactly $|V(k)|/m$ of these orbits have the property that $O$ contains a $k$-rational point (or equivalently all points of $O$ are $k$-rational); thus, the $\gamma$-invariant rational $m$-sets of $V$ that contain at least one $k$-rational point are in 1-1 correspondence with certain subset $Z \subseteq (V/\gamma)(k)$ of cardinality $|V(k)|/m$. Therefore, $\pi$ determines a 1-1 correspondence between $\gamma$-invariant $n$-rational sets of $V$ containing at least one $k$-rational point, and rational $n/m$-sets of $V/\gamma$ containing at least one point of $Z$. Hence,

$$\left|\mathrm{Fix}_\gamma \binom{V}{n}^{\mathrm{rat}}\right| = b_{V/\gamma}\left(\frac{|V(k)|}{m}, \frac{n}{m}\right) = b_V\left(\frac{|V(k)|}{m}, \frac{n}{m}\right).$$

□

In sections 3 and 4 we shall express the number of isomorphism classes of pointed and non-pointed hyperelliptic curves admitting a rational Weierstrass point, in terms of $a_V(n)$ and $b_V(r,n)$ for the varieties

$$V = \mathbb{P}^1,\ \mathbb{A}^1,\ \mathbb{G}_m,\ \mathbb{P}^1_0,$$

where $\mathbb{P}^1_0$ is the subvariety $\mathbb{P}^1 \setminus \{t, t^\sigma\}$, being $t$ any point in $\mathbb{P}^1(k_2) \setminus \mathbb{P}^1(k)$. Formulas for $a_V(n)$ for these four varieties were found in [12, Lem. 2.1] and the value of $b_V(r,n)$ is deduced from Corollary 1.2. Actually, we shall use certain normalizations of these numbers. The following lemma collects all the formulas we need.

**Lemma 1.4.** *For positive integers $n$, $m$ we have*

$$a_{\mathbb{P}^1}(n) = \begin{cases} q^n - q^{n-2}, & \text{if } n \geq 3, \\ q^2, & \text{if } n = 2, \\ q+1, & \text{if } n = 1. \end{cases}$$

$$A_1(n) := \frac{a_{\mathbb{A}^1}(n)}{q} = \begin{cases} q^{n-1} - q^{n-2}, & \text{if } n \geq 2, \\ 1, & \text{if } n = 1. \end{cases}$$

$$A_2(n) := \frac{a_{\mathbb{G}_m}(n)}{q-1} = \frac{q^n - (-1)^n}{q+1}.$$

$$A_0(n) := \frac{a_{\mathbb{P}^1_0}(n)}{q+1} = \frac{q^{n+1} - q^n - (-1)^{\lceil n/2 \rceil} q + (-1)^{\lceil (n-1)/2 \rceil}}{q^2+1}.$$

$$B(n) := \frac{b_{\mathbb{P}^1}(n)}{q(q-1)(q+1)} = \sum_{i=1}^{n-3} (-1)^{i+1} \left(\!\!\binom{q+1}{i}\!\!\right) q^{n-3-i} - \\ - (-1)^n \frac{n-1}{n(q+1)} \left(\!\!\binom{q+1}{n-2}\!\!\right), \quad \forall n > 3.$$

$$B_0(m,n) := \frac{1}{q+1} b_{\mathbb{P}^1_0}\left(\frac{q+1}{m}, n\right) = \\ = \sum_{i=1}^{n-1} (-1)^{i+1} \left(\!\!\binom{(q+1)/m}{i}\!\!\right) A_0(n-i) - \frac{(-1)^n}{q+1} \left(\!\!\binom{(q+1)/m}{n}\!\!\right).$$

$$B_1(n) := \frac{1}{q} b_{\mathbb{A}^1}\left(\frac{q}{p}, n\right) = \\ = \sum_{i=1}^{n-1} (-1)^{i+1} \left(\!\!\binom{q/p}{i}\!\!\right) A_1(n-i) - \frac{(-1)^n}{q} \left(\!\!\binom{q/p}{n}\!\!\right).$$

$$B_2(m,n) := \frac{1}{q-1} b_{\mathbb{G}_m}\left(\frac{q-1}{m}, n\right) = \\ = \sum_{i=1}^{n-1} (-1)^{i+1} \left(\!\!\binom{(q-1)/m}{i}\!\!\right) A_2(n-i) - \frac{(-1)^n}{q-1} \left(\!\!\binom{(q-1)/m}{n}\!\!\right).$$

## 2. Classification of hyperelliptic curves up to $k$-isomorphism

In this section we recall the connection between rational sets of $\mathbb{P}^1$ and hyperelliptic curves over $k$. For generalities on hyperelliptic curves we address the reader to [15, Sec.1].

From now on we assume that $n = 2g + 2$, where $g$ is a positive integer, $g > 1$. To each rational $n$-set $S$ of $\mathbb{P}^1$ we can attach the monic separable polynomial $f_S(x) \in k[x]$ of degree $n$ or $n - 1$ given by:

$$f_S(x) := \prod_{t\in S,\ t\neq\infty} (x - t).$$

To every $\lambda \in k^*$, $S \in \binom{\mathbb{P}^1}{n}(k)$, we can attach the hyperelliptic curve $C_{\lambda,S}$ determined by the Weierstrass equation $y^2 = \lambda f_S(x)$.

For any $\mu \in k^*$ the morphism $(x, y) \mapsto (x, \mu y)$ sets a $k$-isomorphism between $C_{\lambda,S}$ and $C_{\lambda\mu^2,S}$. Thus, if we let the pairs $(\lambda, S)$ run on the set

$$(\lambda, S) \in \mathcal{X}_n := \left(k^*/(k^*)^2\right) \times \binom{\mathbb{P}^1}{n}(k),$$

the curves $C_{\lambda,S}$ contain representatives of all $k$-isomorphism classes of hyperelliptic curves of genus $g$.

The natural action of $\mathrm{PGL}_2(k)$ on $n$-sets of $\mathbb{P}^1$ determines a natural action of $\mathrm{PGL}_2(k)$ on the set of hyperelliptic curves defined over $k$. In order to recall this action we introduce multipliers $J(\gamma, S) \in k^*$ that depend in principle on the choice of a representative in $\mathrm{GL}_2(k)$ of $\gamma \in \mathrm{PGL}_2(k)$. Consider a matrix

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k).$$

For any $t \in \mathbb{P}^1(\overline{k})$ we can define a local multiplier $j(\gamma, t) \in \overline{k}^*$ by

$$j(\gamma, t) := \begin{cases} \det(\gamma)(ct + d)^{-1} & \text{if } t \neq \infty,\ t \neq -d/c \\ c & \text{if } t = -d/c,\ c \neq 0 \\ d & \text{if } t = \infty,\ c = 0 \\ -\det(\gamma)c^{-1} & \text{if } t = \infty,\ c \neq 0 \end{cases}$$

For any rational $n$-set $S$ of $\mathbb{P}^1$ we define a global multiplier

$$J(\gamma, S) := \prod_{t\in S} j(\gamma, t) \in k^*.$$

There is a well-defined action of $\mathrm{PGL}_2(k)$ on the set $\mathcal{X}_n$:

$$\gamma(\lambda, S) := (\lambda J(\gamma, S), \gamma(S)),$$

which is independent of the choice of a representative of $\gamma \in \mathrm{PGL}_2(k)$ in $\mathrm{GL}_2(k)$. The map $(\lambda, S) \mapsto C_{\lambda,S}$ induces a 1-1 correspondence

$$\mathrm{PGL}_2(k)\backslash\mathcal{X}_n \longrightarrow \mathcal{H}_g,$$

where $\mathcal{H}_g$ is the set of $k$-isomorphism classes of hyperelliptic curves over $k$ of genus $g$ [15, Thm.2.4].

Let us adapt this result to the situation we are dealing with in this paper. Recall that a *pointed hyperelliptic curve* is for us a pair $(C, P)$ where $C$ is a hyperelliptic curve over $k$ and $P$ is a rational Weierstrass point of $C$. We say that two pointed curves $(C,P)$, $(C',P')$ are $k$-isomorphic if there is a $k$-isomorphism between $C$ and $C'$ sending $P$ to $P'$. Denote by $\mathcal{H}_g^\bullet$ the set of $k$-isomorphism classes of pointed hyperelliptic curves of genus $g$. On the other hand, denote by $\mathcal{H}_g^{\mathrm{rat}}$ the set of $k$-isomorphism classes of hyperelliptic curves of genus $g$ admitting at least one rational Weierstrass point.

Consider the sets

$$\mathcal{Y}_n := \left(k^*/(k^*)^2\right) \times \binom{\mathbb{P}^1}{n}^{\infty}, \qquad \mathcal{Z}_n := \left(k^*/(k^*)^2\right) \times \binom{\mathbb{P}^1}{n}^{\mathrm{rat}}.$$

These subsets of $\mathcal{X}_n$ are stable under the action of $\mathrm{PGL}_2(k)$. Moreover, the set $\mathcal{Y}_n$ is stable under the action of the affine subgroup, which is the stabilizer of the point $\infty \in \mathbb{P}^1(k)$:

$$\mathrm{Aff}_2(k) := \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \;\Big|\; (a,b) \in k^* \times k \right\} \subseteq \mathrm{PGL}_2(k).$$

The following result is an immediate consequence of [15, Thm.2.4].

**Theorem 2.1.** *The map $(\lambda, S) \mapsto C_{\lambda,S}$ induces 1-1 correspondences*

$$\mathrm{Aff}_2(k)\backslash\mathcal{Y}_n \longrightarrow \mathcal{H}_g^\bullet, \qquad \mathrm{PGL}_2(k)\backslash\mathcal{Z}_n \longrightarrow \mathcal{H}_g^{\mathrm{rat}}.$$

After this result the aim of the paper is to find closed formulas for the cardinalities of the two sets $\mathrm{Aff}_2(k)\backslash\mathcal{Y}_n$, $\mathrm{PGL}_2(k)\backslash\mathcal{Z}_n$. To this end we need the computation of the class of $J(\gamma, S)$ modulo squares given in [15, Thm.3.4], which we recall in Theorem 2.3 below.

Denote by $\epsilon$ the map

$$\epsilon\colon\ \mathrm{PGL}_2(k) \times \binom{\mathbb{P}^1}{n}(k) \xrightarrow{\ J\ } k^*/(k^*)^2 \longrightarrow \{\pm 1\},$$

where the last map is the unique non-trivial group homomorphism between these two groups of order two. We want to compute $\epsilon(\gamma, S)$ for $\gamma$ running on a system of representatives of conjugacy classes of $\mathrm{PGL}_2(k)$, and $S$ a rational $n$-set of $\mathbb{P}^1$ fixed by $\gamma$: $\gamma(S) = S$.

Let us recall how these representatives can be chosen, the possible values of the order $m$ of $\gamma$ in each conjugacy class, the number of representatives of a given order and the cardinality of the centralizers

$$\Gamma_\gamma := \{\rho \in \mathrm{PGL}_2(k) \mid \rho^{-1}\gamma\rho = \gamma\}.$$

The following result is extracted from [13, Prop.2.3, Lem.2.4].

**Lemma 2.2.** *There are $q+2$ conjugacy classes in $\mathrm{PGL}_2(k)$, which we distribute in four types:*

*A. The identity, $\gamma(t) = t$, has order $m = 1$ and $|\Gamma_\gamma| = |\mathrm{PGL}_2(k)| = q(q-1)(q+1)$.*

*B. The translation $\gamma_0(t) = t + 1$. It has $\mathrm{Fix}_{\gamma_0} = \{\infty\}$, order $m = p$ and $|\Gamma_{\gamma_0}| = q$.*

*C. The homothetic automorphisms (conjugate to $t \mapsto \lambda t$, for some $\lambda \in k^*$, $\lambda \neq 1$). They have two fixed points, lying in $\mathbb{P}^1(k)$, and order $m = \mathrm{ord}_{k^*}(\lambda)$, which is a divisor of $q-1$.*

*There are $(q-1)/2$ homothetic conjugacy classes. For any divisor $m>1$ of $q-1$, if $\mathcal{C}_m$ is a system of representatives of the homothetic conjugacy classes of order $m$, we have*

$$\sum_{\gamma\in\mathcal{C}_m} |\Gamma_\gamma|^{-1} = \frac{\varphi(m)}{2(q-1)}.$$

*D. The potentially homothetic automorphisms; i.e. those $\gamma$ conjugate to the class in $\mathrm{PGL}_2(k)$ of a matrix $\begin{pmatrix} 0 & 1 \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k)$ with eigenvalues $\alpha$, $\alpha^\sigma$ in $k_2 \setminus k$. They have two fixed points, which are quadratic conjugate points in $\mathbb{P}^1(k_2)$; the order is the least positive integer $m$ such that $\alpha^m \in k$, and it is a divisor of $q+1$.*

*There are $(q+1)/2$ potentially homothetic conjugacy classes. For any divisor $m>1$ of $q+1$, if $\mathcal{C}_m$ is a system of representatives of the potentially homothetic conjugacy classes of order $m$, we have*

$$\sum_{\gamma\in\mathcal{C}_m} |\Gamma_\gamma|^{-1} = \frac{\varphi(m)}{2(q+1)}.$$

**Theorem 2.3.** *Let $n$ be an even positive integer, $S$ a rational $n$-set of $\mathbb{P}^1$, and $\gamma \in \mathrm{PGL}_2(k)$ an automorphism of $\mathbb{P}^1$ of order $m$ such that $\gamma(S) = S$. Then,*

$$\epsilon(\gamma, S) = \begin{cases} 1, & \text{if } \gamma = 1 \text{ or } \gamma = \gamma_0 \\ (-1)^{(q-1)/m}, & \text{if } \gamma \text{ homothetic and } \infty \in S \\ 1, & \text{if } \gamma \text{ homothetic and } \infty \notin S \\ (-1)^{(q+1)/m}(-1)^{(n-2)/m}, & \text{if } \gamma \text{ pot. homothetic and } \mathrm{Fix}_\gamma \subseteq S \\ (-1)^{n/m}, & \text{if } \gamma \text{ pot. homothetic and } \mathrm{Fix}_\gamma \not\subseteq S \end{cases}$$

## 3. Counting pointed hyperelliptic curves

Let $\Gamma$ be a finite group acting on a finite set $X$. The number of orbits of this action can be counted as the average number of fixed points:

$$|\Gamma\backslash X| = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma} |\operatorname{Fix}_\gamma X| = \sum_{\gamma\in\mathcal{C}} \frac{|\operatorname{Fix}_\gamma X|}{|\Gamma_\gamma|}, \tag{4}$$

where $\mathcal{C}$ is a set of representatives of conjugacy classes of elements of $\Gamma$ and

$$\operatorname{Fix}_\gamma X := \{x \in X \mid \gamma(x) = x\}, \quad \Gamma_\gamma := \{\rho \in \Gamma \mid \rho\gamma\rho^{-1} = \gamma\}.$$

In this section we apply this formula to compute the number $\mathrm{hyp}^\bullet(g)$ of orbits of the set

$$X = \mathcal{Y} := \mathcal{Y}_{2g+2} = \left(k^*/(k^*)^2\right) \times \binom{\mathbb{P}^1}{2g+2}^{\infty}$$

under the action of the affine group $\Gamma := \mathrm{Aff}_2(k)$. By Theorem 2.1 this is the number of $k$-isomorphism classes of pointed hyperelliptic curves of genus $g$: $\mathrm{hyp}^\bullet(g) = |\mathcal{H}_g^\bullet|$.

The following lemma exhibits a system of representatives of conjugacy classes of the affine group:

**Lemma 3.1.** *There are $q$ conjugacy classes in $\operatorname{Aff}_2(k)$, represented by the following elements, which we distribute in three types:*

*A. The identity, $\gamma(t)=t$, has order $m=1$ and $|\Gamma_\gamma|=|\operatorname{Aff}_2(k)|=q(q-1)$.*

*B. The translation $\gamma_0(t)=t+1$. It has $\operatorname{Fix}_{\gamma_0}=\{\infty\}$, order $m=p$ and $|\Gamma_{\gamma_0}|=q$.*

*C. The homotheties $\gamma(t)=\lambda t$, $\lambda\in k^*$, $\lambda\ne 1$. They have $\operatorname{Fix}_\gamma=\{\infty,0\}$, order $m=\operatorname{ord}_{k^*}(\lambda)$, which is a divisor of $q-1$, and $|\Gamma_\gamma|=q-1$.*

*In particular, for any divisor $m>1$ of $q-1$ there are $\varphi(m)$ conjugacy classes in $\operatorname{Aff}_2(k)$ of order $m$.*

For any $\gamma\in\operatorname{Aff}_2(k)$, a pair $(\lambda,S)\in\mathcal{Y}$ is fixed by $\gamma$ if and only if $\gamma(S)=S$ and $\epsilon(\gamma,S)=1$. Thus,

$$|\operatorname{Fix}_\gamma\mathcal{Y}|=2\left|\left\{S\in\operatorname{Fix}_\gamma\left(\begin{array}{c}\mathbb{P}^1\\2g+2\end{array}\right)^{\infty}\;\middle|\;\epsilon(\gamma,S)=1\right\}\right|.$$

By Theorem 2.3, $|\operatorname{Fix}_\gamma\mathcal{Y}|=0$ if $\gamma$ is an homothety of order $m$ with $(q-1)/m$ odd, and

$$|\operatorname{Fix}_\gamma\mathcal{Y}|=2\left|\operatorname{Fix}_\gamma\left(\begin{array}{c}\mathbb{P}^1\\2g+2\end{array}\right)^{\infty}\right|=2\left|\operatorname{Fix}_\gamma\left(\begin{array}{c}\mathbb{A}^1\\2g+1\end{array}\right)(k)\right|,$$

otherwise. We can apply now Theorem 1.3 to compute the number of rational $(2g+1)$-sets of $\mathbb{A}^1$ which are $\gamma$-invariant. If $\gamma$ is an homothety, in order to be able to apply Theorem 1.3 we split these rational $(2g+1)$-sets into two disjoint groups according to the fact that they contain 0 or not; we get in this case

$$\left|\operatorname{Fix}_\gamma\left(\begin{array}{c}\mathbb{A}^1\\2g+1\end{array}\right)(k)\right|=\left|\operatorname{Fix}_\gamma\left(\begin{array}{c}\mathbb{G}_m\\2g\end{array}\right)(k)\right|+\left|\operatorname{Fix}_\gamma\left(\begin{array}{c}\mathbb{G}_m\\2g+1\end{array}\right)(k)\right|,$$

and we obtain

$$\left|\operatorname{Fix}_\gamma\left(\begin{array}{c}\mathbb{A}^1\\2g+1\end{array}\right)(k)\right|=\begin{cases}a_{\mathbb{A}^1}(2g+1), & \text{if } \gamma=1,\\ a_{\mathbb{A}^1}((2g+1)/p), & \text{if } \gamma=\gamma_0,\\ a_{\mathbb{G}_m}(2g/m)+a_{\mathbb{G}_m}((2g+1)/m), & \text{otherwise,}\end{cases}$$

where $m$ is the order of $\gamma$.

The computation of $\operatorname{hyp}^\bullet(g)$ given by (4) can be splitted into the sum of three terms $h_A+h_B+h_C$, each term taking care of the contribution of all conjugacy classes in a concrete type, as described in Lemma 3.1. Since the value of $|\operatorname{Fix}_\gamma\mathcal{Y}|$ depends only on $m$, for the computation of $h_C$ we can group together all $\gamma$ with the same order and we obtain

$$\begin{aligned}\mathrm{hyp}^{\bullet}(g) &= \frac{2a_{\mathbb{A}^1}(2g+1)}{q(q-1)} + \frac{2}{q}a_{\mathbb{A}^1}\left(\frac{2g+1}{p}\right) + \\ &+ \frac{2}{q-1}\sum_{1<m\mid(q-1)/2}\varphi(m)\left(a_{\mathbb{G}_m}\left(\frac{2g}{m}\right) + a_{\mathbb{G}_m}\left(\frac{2g+1}{m}\right)\right) = \\ &= 2q^{2g-1} + 2A_1\left(\frac{2g+1}{p}\right) + \\ &+ \sum_{1<m\mid(q-1)/2} 2\varphi(m)\left(A_2\left(\frac{2g}{m}\right) + A_2\left(\frac{2g+1}{m}\right)\right).\end{aligned}$$

By using the explicit formulas for $A_1(n)$, $A_2(n)$ given in Lemma 1.4 we obtain a closed formula for $\mathrm{hyp}^{\bullet}(g)$ as a polynomial in $q$ with integer coefficients that depend on $g$ and the set of divisors of $q-1$. This is more clearly seen if we rewrite our formula for $\mathrm{hyp}^{\bullet}(g)$ in a way that is more suitable for an effective computation when $g$ is given and we want to deal with a generic value of $q$.

**Theorem 3.2.** *The number of $k$-isomorphism classes of pointed hyperelliptic curves of genus $g$ is:*

$$\begin{aligned}&\mathrm{hyp}^{\bullet}(g) = 2q^{2g-1} + 2A_1\left(\frac{2g+1}{p}\right) + \\ &+ \sum_{1<m\mid 2g+1} 2\varphi(m)\left[A_2\left(\frac{2g+1}{m}\right)\right]_{m\mid q-1} + \sum_{1<m\mid 2g} 2\varphi(m)\left[A_2\left(\frac{2g}{m}\right)\right]_{2m\mid q-1}.\end{aligned}$$

*By convention, $A_1(x) = 0$ if $x$ is not a positive integer and the terms $[x]_{condition}$ are considered only if the "condition" is satisfied.*

We display in Table 1 the value of $\mathrm{hyp}^{\bullet}(g)$ for $2 \le g \le 7$.

**Corollary 3.3.** *The dominant terms of* $\mathrm{hyp}^{\bullet}(g)$ *are*

$$\mathrm{hyp}^{\bullet}(g) = 2q^{2g-1} + O(q^{g-1}).$$

*Proof.* Apart from the generic term $2q^{2g-1}$, the highest power of $q$ arising from the other terms is the degree of $[A_2(g)]_{4\mid q-1}$, corresponding to the divisor $m = 2$ of $2g$. □

## 4. Counting hyperelliptic curves with a rational Weierstrass point

In this section we apply the formula (4) to compute the number $\mathrm{hyp}^{\mathrm{rat}}(g)$ of orbits of the set

$$X = \mathcal{Z} := \mathcal{Z}_{2g+2} = \left(k^*/(k^*)^2\right) \times \left(\begin{array}{c}\mathbb{P}^1\\ 2g+2\end{array}\right)^{\mathrm{rat}}$$

under the action of the projective group $\Gamma := \mathrm{PGL}_2(k)$. By Theorem 2.1 this is the number of $k$-isomorphism classes of hyperelliptic curves of genus $g$ having at least one rational Weierstrass point: $\mathrm{hyp}^{\mathrm{rat}}(g) = |\mathcal{H}_g^{\mathrm{rat}}|$.

TABLE 1. Number of pointed hyperelliptic curves of genus $g$ up to $k$-isomorphism

| $g$ | $\mathrm{hyp}^\bullet(g) = \lvert\mathcal{H}_g^\bullet\rvert$ |
|---|---|
| 2 | $2q^3+2[q-1]_{4\mid q-1}+[4]_{8\mid q-1}+[8]_{5\mid q-1}+[2]_{p=5}$ |
| 3 | $2q^5+2[q^2-q+1]_{4\mid q-1}+4[q-1]_{3\mid q-1}+[12]_{7\mid q-1}+[4]_{12\mid q-1}+[2]_{p=7}$ |
| 4 | $2q^7+2[q^3-q^2+q-1]_{4\mid q-1}+4[q^2-q+1]_{3\mid q-1}+4[q-1]_{8\mid q-1}+$ $+[12]_{9\mid q-1}+[8]_{16\mid q-1}+2[q^2-q]_{p=3}$ |
| 5 | $2q^9+2[q^4-q^3+q^2-q+1]_{4\mid q-1}+8[q-1]_{5\mid q-1}+[20]_{11\mid q-1}+[8]_{20\mid q-1}+$ $+[2]_{p=11}$ |
| 6 | $2q^{11}+2[q^5-q^4+q^3-q^2+q-1]_{4\mid q-1}+4[q^3-q^2+q-1]_{3\mid q-1}+$ $+4[q^2-q+1]_{8\mid q-1}+4[q-1]_{12\mid q-1}+[24]_{13\mid q-1}+[8]_{24\mid q-1}+[2]_{p=13}$ |
| 7 | $2q^{13}+2[q^6-q^5+q^4-q^3+q^2-q+1]_{4\mid q-1}+4[q^4-q^3+q^2-q+1]_{3\mid q-1}+$ $+8[q^2-q+1]_{5\mid q-1}+12[q-1]_{7\mid q-1}+[16]_{15\mid q-1}+[12]_{28\mid q-1}+$ $+2[q^4-q^3]_{p=3}+2[q^2-q]_{p=5}$ |

We divide the conjugacy classes of $\mathrm{PGL}_2(k)$ into four types A, B, C, D, as indicated in Lemma 2.2. The computation of $\mathrm{hyp}^{\mathrm{rat}}(g)$ given by (4) can be splitted into the sum of four terms $\mathrm{hyp}^{\mathrm{rat}}(g) = h_A+h_B+h_C+h_D$, taking care of the contribution of all conjugacy classes of each concrete type.

For any $\gamma \in \mathrm{PGL}_2(k)$, a pair $(\lambda, S) \in \mathcal{Z}$ is fixed by $\gamma$ if and only if $\gamma(S) = S$ and $\epsilon(\gamma, S) = 1$. Thus,

$$|\mathrm{Fix}_\gamma \mathcal{Z}| = 2\left|\left\{S \in \mathrm{Fix}_\gamma \binom{\mathbb{P}^1}{2g+2}^{\mathrm{rat}} \;\Big|\; \epsilon(\gamma,S)=1\right\}\right|.$$

For $\gamma = 1$ and $\gamma = \gamma_0$ Theorem 2.3 shows that $\epsilon(\gamma, S) = 1$ for all $\gamma$-invariant rational $(2g+2)$-sets of $\mathbb{P}^1$. Thus,

$$|\mathrm{Fix}_\gamma \mathcal{Z}| = 2\left|\mathrm{Fix}_\gamma \binom{\mathbb{P}^1}{2g+2}^{\mathrm{rat}}\right|.$$

For $\gamma = 1$ we get directly

$$h_A = \frac{|\mathcal{Z}|}{q(q-1)(q+1)} = \frac{2b_{\mathbb{P}^1}(2g+2)}{q(q-1)(q+1)} = 2B(2g+2).$$

We split the $\gamma_0$-invariant rational $(2g+2)$-sets of $\mathbb{P}^1$ that contain at least one rational point into two families: those containing $\infty$ and those not containing $\infty$. We have,

$$\left|\mathrm{Fix}_{\gamma_0} \binom{\mathbb{P}^1}{2g+2}^{\mathrm{rat}}\right| = \left|\mathrm{Fix}_{\gamma_0} \binom{\mathbb{A}^1}{2g+1}(k)\right| + \left|\mathrm{Fix}_{\gamma_0} \binom{\mathbb{A}^1}{2g+2}^{\mathrm{rat}}\right|.$$

Theorem 1.3 can be applied to compute the cardinality of both families, and we get

$$h_B=\frac{|\operatorname{Fix}_{\gamma_0}\mathcal{Z}|}{q}=\frac{2}{q}\left(a_{\mathbb{A}^1}\left(\frac{2g+1}{p}\right)+b_{\mathbb{A}^1}\left(\frac{q}{p},\frac{2g+2}{p}\right)\right)=$$
$$=2A_1\left(\frac{2g+1}{p}\right)+2B_1\left(\frac{2g+2}{p}\right).$$

For $\gamma$ of type C or D we shall see below that the value of $|\operatorname{Fix}_\gamma\mathcal{Z}|$ depends only on the order $m$ of $\gamma$; hence, in the computation of $h_C$ and $h_D$ we can group together all $\gamma$ with the same order and Lemma 2.2 shows that we can express the partial sums $h_C$ and $h_D$ as:

$$h_C=\sum_{1<m|(q-1)}\frac{\varphi(m)|\operatorname{Fix}_\gamma\mathcal{Z}|}{2(q-1)},\quad h_D=\sum_{1<m|(q+1)}\frac{\varphi(m)|\operatorname{Fix}_\gamma\mathcal{Z}|}{2(q+1)},$$

where for each $m$ we choose an arbitrary $\gamma$ of order $m$ of type C or D.

For $\gamma$ an homothety of order $m$, we split the $\gamma$-invariant rational $(2g+2)$-sets of $\mathbb{P}^1$ that contain at least one rational point into three families: those containing both fixed points of $\gamma$ ($0$ and $\infty$), those containing exactly one fixed point of $\gamma$, and those containing no fixed points of $\gamma$. Since any $\gamma$-invariant $n$-set of $\mathbb{G}_m$ has necessarily $n$ multiple of $m$, Theorem 2.3 shows that:

$$|\operatorname{Fix}_\gamma\mathcal{Z}|=2\left|\operatorname{Fix}_\gamma\binom{\mathbb{G}_m}{2g+2}^{\mathrm{rat}}\right|,\qquad\text{if }\frac{q-1}{m}\text{ odd},$$

$$|\operatorname{Fix}_\gamma\mathcal{Z}|=2\left|\operatorname{Fix}_\gamma\binom{\mathbb{G}_m}{2g}(k)\right|+4\left|\operatorname{Fix}_\gamma\binom{\mathbb{G}_m}{2g+1}(k)\right|+$$
$$+2\left|\operatorname{Fix}_\gamma\binom{\mathbb{G}_m}{2g+2}^{\mathrm{rat}}\right|,\qquad\text{if }\frac{q-1}{m}\text{ even}.$$

Theorem 1.3 can be applied to compute the cardinality of each family, and we get

$$h_C=\sum_{1<m|q-1}\frac{\varphi(m)}{q-1}\left(\left[a_{\mathbb{G}_m}\left(\frac{2g}{m}\right)\right]_{2m|q-1}+2a_{\mathbb{G}_m}\left(\frac{2g+1}{m}\right)+\right.$$
$$\left.+b_{\mathbb{G}_m}\left(\frac{q-1}{m},\frac{2g+2}{m}\right)\right)=\sum_{1<m|q-1}\varphi(m)\left(\left[A_2\left(\frac{2g}{m}\right)\right]_{2m|q-1}+\right.$$
$$\left.+2A_2\left(\frac{2g+1}{m}\right)+B_2\left(\frac{q-1}{m},\frac{2g+2}{m}\right)\right).$$

Finally, $h_D$ can be computed by using completely analogous arguments:

$$h_D = \sum_{1<m|q+1} \frac{\varphi(m)}{q+1}\left(\left[b_{\mathbb{P}^1_0}\left(\frac{q+1}{m},\frac{2g}{m}\right)\right]_{\frac{2g}{m}\equiv\frac{q+1}{m}\ (\mathrm{mod}\ 2)} + \right.$$
$$\left. + \left[b_{\mathbb{P}^1_0}\left(\frac{q+1}{m},\frac{2g+2}{m}\right)\right]_{m|g+1}\right) =$$
$$= \sum_{1<m|q+1} \varphi(m)\left(\left[B_0\left(m,\frac{2g}{m}\right)\right]_{\frac{2g}{m}\equiv\frac{q+1}{m}\ (\mathrm{mod}\ 2)} + \right.$$
$$\left. + \left[B_0\left(m,\frac{2g+2}{m}\right)\right]_{m|g+1}\right).$$

By using the explicit formulas for $A_i(n)$ and $B_i(m,n)$ given in Lemma 1.4 we obtain a closed formula for $\mathrm{hyp}^{\mathrm{rat}}(g)$ as a polynomial in $q$ with rational coefficients that depend on the set of divisors of $q-1$ and $q+1$. As in the previous section we rewrite our computation of $\mathrm{hyp}^{\mathrm{rat}}(g)$ in a way that is more suitable for an effective computation when $g$ is given and we want to deal with a generic value of $q$.

**Theorem 4.1.** *The number of $k$-isomorphism classes of hyperelliptic curves of genus $g$ having at least one rational Weierstrass point is:*

$$\mathrm{hyp}^{\mathrm{rat}}(g) = 2B(2g+2) + 2A_1\left(\frac{2g+1}{p}\right) + 2B_1\left(\frac{2g+2}{p}\right) +$$
$$+ \sum_{1<m|2g} \varphi(m)\left(\left[B_0\left(m,\frac{2g}{m}\right)\right]_{m|q+1,\ \frac{2g}{m}\equiv\frac{q+1}{m}\ (\mathrm{mod}\ 2)} + \left[A_2\left(\frac{2g}{m}\right)\right]_{2m|q-1}\right) +$$
$$+ \sum_{1<m|2g+1} 2\varphi(m)\left[A_2\left(\frac{2g+1}{m}\right)\right]_{m|q-1} +$$
$$+ \sum_{1<m|2g+2} \varphi(m)\left(\left[B_0\left(m,\frac{2g+2}{m}\right)\right]_{m|q+1,\ m|g+1} + \right.$$
$$\left. + \left[B_2\left(m,\frac{2g+2}{m}\right)\right]_{m|q-1}\right).$$

*By convention, $A_1(x) = 0 = B_1(x)$ if $x$ is not a positive integer and the terms $[x]_{condition}$ are considered only if the "condition" is satisfied.*

We display in Table 2 the value of $\mathrm{hyp}^{\mathrm{rat}}(g)$ for $2 \le g \le 5$.

**Corollary 4.2.** *The dominant term of* $\mathrm{hyp}^{\mathrm{rat}}(g)$ *is*

$$\mathrm{hyp}^{\mathrm{rat}}(g) = \left(1 - \frac{1}{2!} + \frac{1}{3!} - \cdots - \frac{1}{(2g+2)!}\right) 2q^{2g-1} + O(q^{2g-2}).$$

*In particular, for $g$ large* $\mathrm{hyp}^{\mathrm{rat}}(g)$ *is asymptotically* $(1-e^{-1})2q^{2g-1}$.

*Proof.* The dominant term is the principal monomial of $2B(2g+2)$. ∎

TABLE 2. Number of hyperelliptic curves of genus $g$ admitting a Koblitz model, up to $k$-isomorphism

| $g$ | $\mathrm{hyp}^{\mathrm{rat}}(g) = \lvert\mathcal{H}_g^{\mathrm{rat}}\rvert$ |
|---|---|
| 2 | $\frac{91}{72}q^3 + \frac{37}{48}q^2 - \frac{1}{2}q + \frac{11}{16} + [q-1]_{4\mid q-1} + \frac{1}{8}[3q+1]_{4\mid q+1} + [2]_{p=5} + [8]_{5\mid q-1} +$ $+[2]_{8\mid q-1} - \left[\frac{2}{9}\right]_{3\mid q-1} + \left[\frac{5}{9}\right]_{3\mid q+1} + \left[\frac{1}{2}\right]_{8\mid q-3}$ |
| 3 | $\frac{3641}{2880}q^5 + \frac{53}{144}q^4 + \frac{83}{144}q^3 - \frac{8}{9}q^2 + \frac{893}{960}q - \frac{3}{8} + [\frac{67}{48}q^2 - \frac{4}{3}q - \frac{7}{16}]_{4\mid q-1} +$ $+2[q-1]_{3\mid q-1} + \frac{1}{9}[5q+2]_{3\mid q+1} + [12]_{7\mid q-1} + [2]_{p=7} + [2]_{12\mid q-1} +$ $+\left[\frac{1}{2}\right]_{8\mid q-1} + \left[\frac{1}{3}\right]_{12\mid q-5}$ |
| 4 | $\frac{28319}{22400}q^7 + \frac{2119}{5760}q^6 - \frac{2059}{9600}q^5 + \frac{6143}{11520}q^4 + \frac{83}{1200}q^3 + \frac{187}{5760}q^2 - \frac{9}{1400}q - \frac{59}{1280} +$ $+\left[-\frac{233}{384}q^3 + \frac{99}{128}q^2 - \frac{607}{384}q + \frac{117}{128}\right]_{4\mid q+1} + 4[q^2-q+1]_{3\mid q-1} + 2[q^2-q]_{p=3} +$ $+2[q-1]_{8\mid q-1} + \frac{1}{16}[7q+3]_{8\mid q+1} + \frac{2}{25}[9q+4]_{5\mid q+1} + \frac{18}{25}[q-1]_{5\mid q-1} +$ $+\left[\frac{9}{25}q - \frac{1}{5}\right]_{p=5} + [12]_{9\mid q-1} + [4]_{16\mid q-1} + \left[\frac{1}{2}\right]_{16\mid q-7}$ |
| 5 | $\frac{27526069}{21772800}q^9 + \frac{16481}{44800}q^8 - \frac{778721}{3628800}q^7 + \frac{11923}{86400}q^6 + \frac{44881}{64800}q^5 - \frac{43909}{43200}q^4 + \frac{3133141}{3628800}q^3 -$ $-\frac{252227}{201600}q^2 + \frac{357221}{161280}q - \frac{171}{256} + \left[\frac{5351}{3840}q^4 - \frac{199}{160}q^3 + \frac{521}{640}q^2 - \frac{391}{240}q + \frac{597}{256}\right]_{4\mid q-1} +$ $+\left[\frac{155}{324}q^2 - \frac{167}{162}q + \frac{137}{972}\right]_{3\mid q+1} - \left[\frac{155}{324}q^2 - \frac{241}{162}q + \frac{1361}{972}\right]_{3\mid q-1} + 4[q-1]_{5\mid q-1} +$ $+\left[\frac{18}{25}q + \frac{8}{25}\right]_{5\mid q+1} + [20]_{11\mid q-1} + [2]_{p=11} + [4]_{20\mid q-1} + \left[\frac{1}{3}\right]_{12\mid q-1} + \left[\frac{2}{5}\right]_{20\mid q-9}$ |

## REFERENCES


[1] Y. Choie, D. Yun, *Isomorphism classes of hyperelliptic curves of genus 2 over* $\mathbb{F}_q$, Proc. of ACISP'02, Lecture Notes in Computer Science **2384** (2002), 190-202.

[2] Y. Choie, E. Jeong, *Isomorphism classes of hyperelliptic curves of genus 2 over* $\mathbb{F}_{2^n}$, Cryptology ePrint Archive 2003/213.

[3] Y. Choie, E. Jeong, *Isomorphism classes of elliptic and hyperelliptic curves over finite fields* $\mathbb{F}_{(2g+1)^n}$, Finite Fields and Their Applications **10** (2004), 583-614.

[4] Y. Deng, M. Liu, *Isomorphism classes of hyperelliptic curves of genus* 2 *over finite fields with characteristic* 2, Sci. China Ser. A **49**(2) (2005), 173-184.

[5] Y. Deng, *Isomorphism classes of hyperelliptic curves of genus* 3 *over finite fields*, Finite Fields and Their Applications **12** (2006), 248-282.

[6] J. Espinosa García, L. Hernández Encinas, J. Muñoz Masqué, *A Review on the isomorphism Classes of hyperelliptic Curves of Genus 2 over Finite Fields Admitting a Weierstrass Point*, Acta Appl. Math **93** (2006), 299-318.

[7] L. Hernández Encinas, A.J. Menezes, J. Muñoz Masqué, *Isomorphism Classes of Genus-2 hyperelliptic Curves over Finite Fields*, Appl. Algebra Engrg. Comm. Comput. **13** (2002), 57-65.

[8] L. Hernández Encinas, J. Muñoz Masqué, *Isomorphism classes of genus-2 hyperelliptic curves over finite fields* $\mathbb{F}_{5^m}$, Information **8**(6), 8pp. (2005).

[9] E. Jeong, *Isomorphism classes of hyperelliptic curves of genus 3 over finite fields*, Cryptology ePrint Archive 2003/251.

[10] N. Koblitz, *Hyperelliptic cryptosystems*, Journal of Cryptology **1** (1989), 139-150.

[11] P. Lockhart, *On the discriminant of a hyperelliptic curve*, Transactions of the American Mathematical Society **342** (1994), 729-752.

[12] A. López, D. Maisner, E. Nart, X. Xarles, Orbits of galois invariant $n$-sets of $\mathbb{P}^1$ under the action of $\mathrm{PGL}_2$, Finite Fields and Their Applications **8** (2002) 193-206.

[13] A. López, E. Nart, *Classification of Goppa codes of genus zero*, Journal für die reine und angewandte Mathematik **517** (1999), 131-144.

[14] R. Martí, E. Nart, *Orbits of rational n-sets of projective spaces under the action of the linear group*, http://www.arxiv.org/math.CO/0701836.

[15] E. Nart, *Counting hyperelliptic curves*, http://www.arxiv.org/math.NT/0703549.