Finite Fields and Their Applications **8,** 193–206 (2002)
doi.10.1006/ffta.2001.0335, available online at http://www.idealibrary.com on IDEAL®

Orbits of Galois Invariant *n*-Sets of $\mathbb{P}^1$ under the Action of PGL_2

Amparo López, Daniel Maisner,[1] Enric Nart, and Xavier Xarles[2]

Departament de Matemàtiques, Universitat Autònoma de Barcelona, 08193 Bellaterra, Barcelona, Spain
E-mail: alopez@mat.uab.es, danielm@mat.uab.es, nart@mat.uab.es, xarles@mat.uab.es

Communicated by Michael Tsfasman

Received October 16, 2000; published online January 30, 2002

For any finite field k we count the number of orbits of galois invariant n-sets of $\mathbb{P}^1(\bar{k})$ under the action of $\mathrm{PGL}_2(k)$. For k of odd characteristic, this counts the number of k-points of the moduli space of hyperelliptic curves of genus g over k. We get in this way an explicit formula for the number of hyperelliptic curves over k of genus g, up to k-isomorphism and quadratic twist. © 2002 Elsevier Science (USA)

Key words: hyperelliptic curves; n-sets of projective spaces.

0. INTRODUCTION

Let $k = \mathbb{F}_q$ be a finite field with q elements. For any positive integer n, the number of orbits of n-sets of $\mathbb{P}^1(k)$ under the action of $\mathrm{PGL}_2(k)$ was counted in [5]. In this way, we get a formula for the number of isometry classes of Goppa codes of genus zero of length n and a fixed dimension r (cf. [7]) or equivalently, for the number of classes modulo the action of $\mathrm{PGL}_r(k)$ of n-arcs in $\mathbb{P}^{r-1}$ whose points lie in a rational normal curve (cf. [4]). It is remarkable that these numbers are independent of r.

On the other hand, there is a well-known connection between n-sets of $\mathbb{P}^1$ and hyperelliptic curves. Consider for any positive integer n the variety

$$\mathcal{M}_n = \binom{\mathbb{P}^1}{n} \backslash \mathrm{PGL}_2.$$

[1]Supported by CONACYT.
[2]Supported by DGI, BHA 2000-0180.

1071-5797/02 $35.00

Then, if the characteristic of k is odd, the variety $\mathscr{M}_{2g+2}$ is a coarse moduli space for hyperelliptic curves of genus g. In this context the formula of [5] certainly counts isomorphy classes of hyperelliptic curves, but only of those curves having all their Weierstrass points defined over k (cf. Section 3).

The aim of this paper is to find a formula for the number of k-points of this variety $\mathscr{M}_n$ for any finite field (of even or odd characteristic) and for any positive integer n. That is, we want to count the cardinal of

$$\mathscr{M}_n(k) = \binom{\mathbb{P}^1(\bar{k})}{n}^{\mathrm{Gal}(\bar{k}/k)} \backslash \mathrm{PGL}_2(k).$$

This is achieved in Section 2, where we prove that for $n > 2$,

$$\begin{aligned}|\mathscr{M}_n(k)| = {} & \frac{1}{2(q+1)} \sum_{e=0}^{2} \binom{2}{e} \sum_{m|(q-1,n-e)} \varphi(m)(q^{(n-e)/m} - (-1)^{(n-e)/m}) \\ & + \frac{1}{q} \sum_{e=0}^{1} \sum_{m|(p,n-e)} (-1)^{\varphi(m^2)}(q^{(n-e)/m} - q^{(n-e)/m-1} + [1]_{n-e=m}) \\ & + \frac{1}{2(q^2+1)} \sum_{e\in\{0,2\}} \sum_{m|(q+1,n-e)} \varphi(m) q(^{((n-e)/m)+1} - q^{(n-e)/m} + (-1)^{[(n-e)/2m]} \\ & + (-1)^{[(n-e-m)/2m]} q),\end{aligned}$$

where φ is Euler's phi function, p is the characteristic of k, and $[1]_{n-e=m}$ means "add 1 if $n - e = m$."

As we explain in Section 3, for $n = 2g + 2 \geq 6$, this formula counts, in the odd characteristic case, the number of hyperelliptic curves of genus g defined over k, up to k-isomorphism and quadratic twist.

In Section 1 we find explicit formulas for the number of points of the discriminant variety, which are used in Section 2 to obtain the above formula.

1. THE DISCRIMINANT VARIETY

Let $n > 1$ be a positive integer and let

$$f(x) = v_n x^n + v_{n-1} x^{n-1} + \cdots v_1 x + v_0$$

be a generic polynomial of degree n. The nth discriminant is an homogeneous polynomial of degree $2n - 2$ in the variables $v_n, \ldots, v_0$, with integral coefficients, defined as

$$D_n(v_n, \dots, v_0) = R(f, f')/v_n,$$

where $R(,)$ denotes the resultant of two polynomials. The following property is easy to check:

$$D_n(0, v_{r-1}, \dots, v_0) = (-1)^{n-1} v_{n-1}^2 D_{n-1}(v_{n-1}, \dots, v_0).$$

Let k be a field and $v_0, v_1, \dots, v_n \in k$. If $v_n \neq 0$, then $D_n(v_n, \dots, v_0) = 0$ if and only if the polynomial $v_n x^n + \cdots + v_0$ has multiple roots.

The *nth discriminant variety* is defined as the projective variety $\Delta \subseteq \mathbb{P}^n$ defined by the equation $D_n(v_n, \dots, v_0) = 0$.

For any $0 \leq i \leq n$, let Z_i be the closed subvariety of $\mathbb{P}^n$ defined by $v_i = 0$ and let $U_i = \mathbb{P}^n - Z_i$. We can express the discriminant variety as the disjoint union, $\Delta = \Delta_1 \cup \Delta_2 \cup \Delta_3$, where

$$\Delta_1 = \Delta \cap U_n, \qquad \Delta_2 = \Delta \cap Z_n \cap U_{n-1}, \qquad \Delta_3 = \Delta \cap Z_n \cap Z_{n-1}.$$

We call Δ_1 the *affine nth discriminant variety*. By the considerations above, the sets of k-points of the three subvarieties $\Delta_1, \Delta_2, \Delta_3$ are in bijection respectively with

$$\Delta_1(k) \leftrightarrow \{\text{inseparable polynomials } x^n + v_{n-1}x^{n-1} + \cdots + v_0 \in k[x]\},$$

$$\Delta_2(k) \leftrightarrow \{\text{inseparable polynomials } x^{n-1} + v_{n-2}x^{n-2} + \cdots + v_0 \in k[x]\},$$

$$\Delta_3(k) \leftrightarrow \mathbb{P}^{n-2}(k).$$

The nth discriminant variety is the dual variety of the rational normal curve C in $\mathbb{P}^n$, with points $P_\infty = (0, \dots, 0, 1)$ and $(1, t, t^2, \dots, t^{n-1})$, $t \in \bar{k}$. Under this point of view, the points of Δ_1 correspond to hyperplanes $v_0 x_0 + \cdots + v_n x_n$ cutting the affine part of C with multiplicity greater than one at some point and not containing P_∞, the points of Δ_2 correspond to hyperplanes cutting the affine part of C with multiplicity greater than one at some point and cutting C with multiplicity one at P_∞, whereas the points of Δ_3 correspond to hyperplanes cutting C with multiplicity greater than one at P_∞.

Our aim in this section is to count, when k is a finite field, the number of k-rational points of the affine and projective discriminant varieties. The variety Δ is birrationally equivalent to $\mathbb{P}^{n-1}$, but it has many singularities, so that it is not clear how could one compute the number of k-points by geometric methods. Nevertheless, as we have seen, this computation amounts to counting the number of inseparable polynomials of a given degree. By unique factorization, it is not difficult to find explicit formulas for the number $s(n)$ of monic separable polynomials of degree n in terms of the numbers N_m of monic irreducible polynomials of degree m. Considering that a polynomial is in a unique way a product of r_1 irreducible polynomials of degree one, r_2 irreducible polynomials of degree two, etc., we have

$$s(n) = \sum_{r_1+2r_2+\cdots+nr_n=n} \binom{N_1}{r_1}\binom{N_2}{r_2}\cdots\binom{N_n}{r_n},$$

understanding that $\binom{N}{r} = 0$ if $N < r$.

However, these kind of formulas where the sum runs over all partitions of n are very unsatisfactory from the combinatorial point of view. The partitions are easy to generate, but we cannot consider that the expression above is quite *explicit* as a closed formula for $s(n)$. In the next theorem we find a very simple computation of $s(n)$.

As a general rule for the rest of the paper, a term $[a]_{b=c}$ in a formula means "add a if $b = c$." Similarly, a term $[a]_{b\equiv c(d)}$ in a formula means "add a if b is congruent to c modulo d."

THEOREM 1.1. *For any positive integer n the number $s(n)$ of monic separable polynomials of degree n with coefficients in $k = \mathbb{F}_q$ is*

$$s(n) = q^n - q^{n-1} + [1]_{n=1}.$$

Proof. Any monic polynomial $t(x)$ of degree n with coefficients in k can be written in a unique way as $t(x) = a(x)^2 b(x)$, where $a(x)$ is a monic polynomial of degree $0 \le r \le [\frac{n}{2}]$ and $b(x)$ is a monic separable polynomial of degree $n-2r$, both $a(x)$ and $b(x)$ with coefficients in k. Hence we have

$$q^n = \sum_{r=0}^{[n/2]} q^r s(n-2r), \tag{1}$$

where we put $s(0) = 1$ understanding that the constant 1 is the unique monic separable polynomial of degree 0.

We can proceed now to prove the theorem by induction on n. For $n = 1$ the assertion $s(1) = q$ is clear. Assume $n > 1$; by (1) and the induction hypothesis we can calculate $s(n)$ as

$$s(n) = q^n - \sum_{r=1}^{[n/2]} q^r s_{n-2r}(q) = q^n - \sum_{r=1}^{[n/2]-1} q^r(q^{n-2r} - q^{n-2r-1}) - q^{[n/2]} s\left(n - 2\left[\frac{n}{2}\right]\right)$$

$$= q^n - q^{n-1} + q^{n-[n/2]} - q^{[n/2]} s\left(n - 2\left[\frac{n}{2}\right]\right).$$

Moreover, in both cases $n = 2r$ even or $n = 2r + 1$ odd we have

$$q^{n-[n/2]} - q^{[n/2]} s\left(n - 2\left[\frac{n}{2}\right]\right) = \begin{cases} q^r - q^r s(0) = 0, & \text{if } n \text{ is even,} \\ q^{r+1} - q^r s(1) = 0, & \text{if } n \text{ is odd.} \end{cases} \qquad \blacksquare$$

COROLLARY 1.1. *For $n > 1$, the number of $\mathbb{F}_q$-points of the affine and projective nth discriminant varieties is*

$$|\Delta_1(\mathbb{F}_q)| = q^{n-1},$$

$$|\Delta(\mathbb{F}_q)| = q^{n-1} + q^{n-2} + [-1]_{n=2} + \frac{q^{n-1} - 1}{q - 1} = \frac{q^n - 1}{q - 1} + q^{n-2} + [-1]_{n=2}.$$

This result suggests that the affine nth discriminant variety could be parameterized by $n - 1$ affine parameters. We have not been able to check this.

2. ORBITS OF GALOIS INVARIANT n-SETS OF $\mathbb{P}^1(\bar{k})$ UNDER THE ACTION OF $\mathrm{PGL}_2(k)$

Let p be a prime number, q a power of p, and $k = \mathbb{F}_q$ the finite field with q elements. We choose a point $\infty \in \mathbb{P}^1(k)$, which we call infinity. This choice determines a k-embedding $\mathbb{A}^1 \hookrightarrow \mathbb{P}^1$, as well as an identification: $\mathrm{Aut}(\mathbb{P}^1) = \mathrm{PGL}_2$. From now on we denote the group $\mathrm{PGL}_2(k)$ simply by Γ. We recall that the galois group $G := \mathrm{Gal}(\bar{k}/k)$ is topologically generated by the Frobenius automorphism F, acting as $x^F = x^q$, for all $x \in \bar{k}$. The group G has a natural action over $\mathbb{P}^1(\bar{k})$ and by our choice we have $\infty^F = \infty$. To say that some object is *galois invariant* or *defined over* k means that it is fixed by all elements of G, or equivalently, that it is fixed by F.

Let us fix throughout a positive integer $n > 2$. The number of orbits of *n-sets of* $\mathbb{P}^1(k)$ under the action of Γ have been counted in [5, Theorem C]. As we explain in Section 3, taking $n = 2g + 2$ one obtains an explicit formula, in the odd characteristic case, for the number of hyperelliptic curves of genus g defined over k having all Weierstrass points defined over k. In order to count all hyperelliptic curves defined over k we have to count orbits under the action of Γ of n-sets of $\mathbb{P}^1(\bar{k})$ which are defined over k (as a set).

Let $\mathscr{X} := \binom{\mathbb{P}^1(\bar{k})}{n}^G$ be the set of galois invariant elements of $\binom{\mathbb{P}^1(\bar{k})}{n}$. The elements of $\mathscr{X}$ are families $\{P_1, \ldots, P_n\}$ of n different points of $\mathbb{P}^1(\bar{k})$ such that

$$\{P_1, \ldots, P_n\} = \{P_1^\sigma, \ldots, P_n^\sigma\}, \qquad \forall \sigma \in G.$$

Our aim is to count the number of orbits of the finite set $\mathcal{X}$ under the action of Γ. To this end we need to consider the following subsets of $\mathcal{X}$,

$$\mathcal{X}_1 = \binom{\mathbb{P}^1(\bar{k}) - \{\infty\}}{n}^G, \qquad \mathcal{X}_2 = \binom{\mathbb{P}^1(\bar{k}) - \{\infty, 0\}}{n}^G,$$

$$\mathcal{X}_0 = \binom{\mathbb{P}^1(\bar{k}) - \{\alpha, \alpha'\}}{n}^G,$$

where $\alpha \in \mathbb{F}_{q^2} - \mathbb{F}_q$ and $\alpha' = \alpha^q$ is the conjugate of α.

We denote the cardinals of these sets by

$$S(n) := |\mathcal{X}|, \qquad S_i(n) := |\mathcal{X}_i|, \quad \text{for } i = 0, 1, 2.$$

To any n-subset $T = \{P_1, \dots, P_n\}$ of $\mathbb{P}^1(\bar{k})$, not containing ∞, we can attach the separable polynomial $f_T(x) = (x - P_1), \dots, (x - P_n)$ and the fact that T is galois invariant is equivalent to $f_T(x)$ having coefficients in k. Needless to say, the n-set T is recovered from $f_T(x)$ as the set of roots in $\bar{k}$ of this polynomial. This correspondence between certain galois invariant subsets of the set of n-sets and certain subsets of separable polynomials with coefficients in k enables us to use Theorem 1.1 to find very explicit formulas for the numbers $S(n)$, $S_i(n)$ as polynomials in q.

LEMMA 2.1. *For any positive integer $n > 1$ we have*:

(1) $S(n) = q^n - q^{n-2} + [1]_{n=2}$,
(2) $S_1(n) = q^n - q^{n-1}$,
(3) $S_2(n) = (q-1)(q^n + (-1)^{n-1})/(q+1)$,
(4) $S_0(n) = (q+1)(q^{n+1} - q^n + (-1)^{[n/2]} + (-1)^{[(n-1)/2}q)/(q^2+1)$.

Proof. The first two assertions are clear. In fact, $s(n)$, (resp. $s(n-1)$) coincides with the number of elements in $\mathcal{X}$ not containing (resp. containing) ∞, so that $S(n) = s(n) + s(n-1)$ and $S_1(n) = s(n)$.

Let us think that $S_2(n)$ is equal to the number of monic separable polynomials of degree n with coefficients in $\mathbb{F}_q$, which are not divisible by x. We prove now (3) for all $n \geq 1$ by induction on n. For $n = 1$ the formula says $S_2(1) = q - 1$, which is true. For $n > 1$ we have $s(n) = S_2(n) + S_2(n-1)$, since each separable polynomial is either not divisible by x or decomposes as $xg(x)$, where $g(x)$ is separable and not divisible by x. Hence, by induction hypothesis,

$$S_2(n) = s(n) - S_2(n-1) = q^n - q^{n-1} - (q-1)(q^{n-1} + (-1)^{n-2})/(q+1)$$

$$= (q-1)(q^n + (-1)^{n-1})/(q+1).$$

Finally, let $q(x) \in k[x]$ be a fixed irreducible quadratic polynomial and let us denote by $s_0(n)$ the number of monic separable polynomials of degree n with coefficients in k and not divisible by $q(x)$. We claim that

$$s_0(n) = \frac{q^{n+2} - q^{n+1} + (-1)^{[n/2]} q^{n-2[n/2]}(q+1)}{q^2+1}, \qquad \forall n \geq 1.$$

Let us prove this by induction on n. For $n = 1$ the formula claims that $s_0(1) = q$, which is true. For $n > 1$ we have as above $s(n) = s_0(n) + s_0(n-2)$, since each separable polynomial is either not divisible by $q(x)$ or decomposes as $q(x)g(x)$, where $g(x)$ is separable and not divisible by $q(x)$. Hence, by induction hypothesis,

$$\begin{aligned} s_0(n) &= q^n - q^{n-1} - \frac{q^n - q^{n-1} + (-1)^{[n/2]-1} q^{n-2[n/2]}(q+1)}{q^2+1} \\ &= \frac{q^{n+2} - q^{n+1} + (-1)^{[n/2]} q^{n-2[n/2]}(q+1)}{q^2+1}, \end{aligned}$$

as claimed. We can now deduce (4) from $S_0(n) = s_0(n-1) + s_0(n)$, since any n-set in $\mathscr{X}_0$ either contains ∞ or not. ■

The main tool in counting $|\mathscr{X} \backslash \Gamma|$ is the following formula, which in [1] is called the Cauchy–Frobenius Lemma,

$$|\mathscr{X} \backslash \Gamma| = \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} |\mathscr{X}_\gamma| = \sum_{\gamma \in \mathscr{C}} \frac{|\mathscr{X}_\gamma|}{|\Gamma_\gamma|},$$

where

$$\mathscr{X}_\gamma = \{T \in \mathscr{X} \,|\, \gamma(T) = T\}, \qquad \Gamma_\gamma = \{\rho \in \Gamma \,|\, \rho\gamma\rho^{-1} = \gamma\},$$

and $\mathscr{C}$ is a system of representatives of conjugation classes of Γ. The set $\mathscr{C}$ and the cardinals $|\Gamma_\gamma|$ are well known. To compute the last sum in the above formula we need also to know for any fixed positive integer m the number of elements in $\mathscr{C}$ of order m as elements of the group Γ. This was computed in [5, Lemma 2.4]. For convenience of the reader we sum up all this information in the following lemma:

LEMMA 2.2. *In the finite field $k = \mathbb{F}_q$ let U_0 be the subset of elements $a \in k^*$ such that the polynomial $x^2 - x - a$ is irreducible over k and let U_2 be a system of representatives of $k^* - \{\pm 1\}$ under the equivalence relation,*

$b \sim b^{-1}$. *Let us consider the following elements and subsets of* Γ:

$$\gamma_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad \Sigma_0 = \left\{ \begin{pmatrix} 0 & a \\ 1 & 1 \end{pmatrix} \middle| \, a \in U_0 \right\}, \qquad \Sigma_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \middle| \, b \in U_2 \right\}.$$

If q *is odd we take also into consideration the following two elements of* Γ,

$$\gamma_0 = \begin{pmatrix} 0 & c \\ 1 & 0 \end{pmatrix}, \qquad \gamma_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

where c *is some fixed non-square in* k. *Then,*

$$\mathscr{C} = \begin{cases} \{1\} \cup \Sigma_0 \cup \Sigma_2 \cup \{\gamma_1\}, & \textit{if } q \textit{ is even}, \\ \{1\} \cup \Sigma_0 \cup \Sigma_2 \cup \{\gamma_0, \gamma_1, \gamma_2\}, & \textit{if } q \textit{ is odd}. \end{cases}$$

For $\gamma \in \Gamma$, $\gamma \neq 1$, *let* $f(\gamma)$ *denote the number of fixed points of* γ *in* $\mathbb{P}^1(k)$. *Then*

$$f(\gamma) = \begin{cases} 0, & \textit{if } \gamma \in \Sigma_0, \textit{ or } \gamma = \gamma_0, \\ 1, & \textit{if } \gamma = \gamma_1, \\ 2, & \textit{if } \gamma \in \Sigma_2, \textit{ or } \gamma = \gamma_2. \end{cases}$$

Moreover,

$$|\Gamma_\gamma| = \begin{cases} q+1, & \textit{if } \gamma \in \Sigma_0, \\ q-1, & \textit{if } \gamma \in \Sigma_2, \\ q, & \textit{if } \gamma = \gamma_1, \\ 2q+2, & \textit{if } \gamma = \gamma_0, \\ 2q-2, & \textit{if } \gamma = \gamma_2. \end{cases}$$

If $m(\gamma)$ *denotes the order of* γ *as an element of* Γ *we have*

$$m(\gamma) = \begin{cases} p, & \textit{if } \gamma = \gamma_1, \\ 2, & \textit{if } \gamma = \gamma_0 \textit{ or } \gamma_2, \\ \textit{a divisor greater than 2 of } q+1, & \textit{if } \gamma \in \Sigma_0, \\ \textit{a divisor greater than 2 of } q-1, & \textit{if } \gamma \in \Sigma_2. \end{cases}$$

Moreover, for any divisor m *of* $q+1$ (*resp.* $q-1$), $m > 2$, *there are exactly* $\varphi(m)/2$ *elements in* Σ_0 (*resp.* Σ_2) *with* $m(\gamma) = m$.

Our aim now is to count $|\mathscr{X}_\gamma|$ for each $\gamma \in \mathscr{C}$. The following observation is useful:

LEMMA 2.3. *Let γ be an element with finite order $m > 1$ in the group Γ and let $P \in \mathbb{P}^1(\bar{k})$. If P is not a fixed point of γ then the orbit of P under the cyclic group $\langle\gamma\rangle$ consists of m different points $P, \gamma(P), \ldots, \gamma^{m-1}(P)$.*

Proof. The jordan normal form of any representative of γ in $\mathrm{GL}_2(k)$ determines if γ has 1 or 2 fixed points in $\mathbb{P}^1(\bar{k})$. It is easy to check that the powers γ^r, $1 \leq r < m$, have a jordan normal form of the same type; hence, all these powers have the same set of fixed points. ■

The crucial result allowing us to count $|\mathscr{X}_\gamma|$ is the following:

THEOREM 2.1. *For any $\gamma \in Aut(\mathbb{P}^1)$ of finite order, the quotient $\mathbb{P}^1 \to \mathbb{P}^1 \backslash \langle\gamma\rangle$ exists in the category of algebraic varieties over k and the quotient variety $\mathbb{P}^1 \backslash \langle\gamma\rangle$ is k-isomorphic to $\mathbb{P}^1$.*

Proof. The existence of the quotient under the action of a finite group is well known [3, Lect. 10]. Moreover, it is easy to check that the quotient of a normal variety is again normal. In our case, the quotient will be a smooth projective curve, which by Lüroth's theorem is birrationally equivalent (thus isomorphic) to $\mathbb{P}^1$. ■

We are ready to give an explicit formula for $|\mathscr{X}_\gamma|$ in terms of the number $f(\gamma)$ of fixed points of γ in $\mathbb{P}^1(k)$ (which can be 0, 1, or 2) and the order $m(\gamma)$ of γ as an element of Γ:

PROPOSITION 2.1. *Let γ be an element of order m in Γ and, for $\gamma \neq 1$, let $f \in \{0, 1, 2\}$ be the number of fixed points of γ in $\mathbb{P}^1(k)$. Then*

$$|\mathscr{X}_\gamma| = \begin{cases} S(n) & \text{if } \gamma = 1, \\[2ex] S_0\left(\dfrac{n}{m}\right) + S_0\left(\dfrac{n-2}{m}\right) & \text{if } f = 0, \\[2ex] S_1\left(\dfrac{n}{m}\right) + S_1\left(\dfrac{n-1}{m}\right) & \text{if } f = 1, \\[2ex] S_2\left(\dfrac{n}{m}\right) + 2S_2\left(\dfrac{n-1}{m}\right) + S_2\left(\dfrac{n-2}{m}\right) & \text{if } f = 2, \end{cases}$$

where we understand that $S_i(x) = 0$ if $x \notin \mathbb{Z}$.

Proof. Let T be a galois invariant n-subset of $\mathbb{P}^1(\bar{k})$ such that $\gamma(T) = T$. We can express T as a disjoint union, $T = T_f \cup T'$, where T_f is the set of all fixed points of γ contained in T and T' is a union of orbits of cardinal m by

Lemma 2.3. Clearly T_f is galois invariant too, hence, it contains either fixed points defined over k, or a pair of quadratic conjugate elements (if $f=0$). On the other hand, T' is also galois invariant and if it has r orbits then it corresponds in a unique way with an r-subset defined over k of the quotient variety $\mathbb{P}^1/\langle\gamma\rangle$. By Theorem 2.1 the number of possibilities for T' is equal to the number of r-subsets defined over k of $\mathbb{P}^1(\bar{k})$ – {fixed points of γ} and these numbers are given by $S_i(r)$, $i=0,1,2$, according to the three different possibilities for the set of fixed points of γ.

The formulas for $|\mathscr{X}_\gamma|$ are obtained by taking into consideration for each possible set T_f the different possibilities for T'. ∎

After this result and Lemma 2.2 we are able to write down an explicit formula for $|\mathscr{X}\backslash\Gamma|$, as the sum of the terms

$$\frac{|\mathscr{X}|}{|\Gamma|}=\frac{S(n)}{q(q-1)(q+1)},$$

$$\frac{|\mathscr{X}_{\gamma_1}|}{|\Gamma_{\gamma_1}|}=\frac{S_1(n/p)+S_1((n-1)/p)}{q},$$

$$\sum_{\gamma\in\mathscr{C},\,f(\gamma)=0}\frac{|\mathscr{X}_\gamma|}{|\Gamma_\gamma|}=\sum_{m|(q+1),m>1}\frac{\varphi(m)}{2}\,\frac{S_0(n/m)+S_0((n-2)/m)}{q+1},$$

$$\sum_{\gamma\in\mathscr{C},\,f(\gamma)=2}\frac{|\mathscr{X}_\gamma|}{|\Gamma_\gamma|}=\sum_{m|(q-1),m>1}\frac{\varphi(m)}{2}\,\frac{S_2(n/m)+2S_2((n-1)/m)+S_2((n-2)/m)}{q-1}.$$

Note that the contributions of γ_0 and γ_2 have been introduced in the last two sums by letting m take the value $m=2$. If q is even, this never happens since m is a divisor of $q+1$ or $q-1$, whereas for q odd, $\varphi(m)/2$ times $1/(q+1)$, resp. $1/(q-1)$, takes for $m=2$ the right value $1/(2q+2)$, resp. $1/(2q-2)$ corresponding to the contribution of γ_0, resp. γ_2.

As a consequence of Lemma 2.1 our formula reads:

THEOREM 2.2 *For $n>2$ a positive integer we have*

$$|\mathscr{X}\backslash\Gamma|=q^{n-3}+\frac{1}{2(q+1)}\sum_{e=0}^{2}\binom{2}{e}\sum_{m|(q-1,n-e),\,m>1}\varphi(m)\,(q^{(n-e)/m}-(-1)^{(n-e)/m})$$
$$+\frac{1}{q}\sum_{e=0}^{1}([q^{(n-e)/p}-q^{(n-e)/p-1}]_{n\equiv e(p)}+[1]_{n-e=p})$$
$$+\frac{1}{2(q^2+1)}\sum_{e\in\{0,2\}}\sum_{m|(q+1,n-e),\,m>1}\varphi(m)(q^{(n-e)/m+1}-q^{(n-e)/m}+(-1)^{[(n-e)/2m]}$$
$$+(-1)^{[(n-e-m)/2m]}q).$$

Remarks 2.1 (1) *It is easy to check that* $|\mathscr{X}\backslash\Gamma| = n$ *for* $n = 1, 2$.
(2) *The term* q^{n-3} *can be expressed as*

$$q^{n-3} = \frac{q^n + 2q^{n-1} + q^{n-2}}{2(q+1)} - \frac{q^n - q^{n-2}}{q} + \frac{q^{n+1} - q^n + q^{n-1} - q^{n-2}}{2(q^2+1)},$$

hence we can obtain a more compact formula just by distributing this term q^{n-3} *among the others, taking into consideration all cases* $m = 1$,

$$|\mathscr{X}\backslash\Gamma| = \frac{1}{2(q+1)} \sum_{e=0}^{2} \binom{2}{e} \sum_{m|(q-1,n-e)} \varphi(m)(q^{(n-e)/m} - (-1)^{(n-e)/m}$$
$$+ \frac{1}{q} \sum_{e=0}^{1} \sum_{m|(p,n-e)} (-1)^{\varphi(m^2)} (q^{(n-e)/m} - q^{(n-e)/m-1} + [1]_{n-e=m})$$
$$+ \frac{1}{2(q^2+1)} \sum_{e\in\{0,2\}} \sum_{m|(q+1,n-e)} \varphi(m)(q^{(n-e)/m+1} - q^{(n-e)/m}$$
$$+ (-1)^{[(n-e)/2m]} + (-1)^{[(n-e-m)/2m]}q).$$

3. COUNTING HYPERELLIPTIC CURVES

As a general reference for the basic properties of hyperelliptic curves see [2, 6]. Let k be a perfect field of characteristic different from 2. Let $f(x) = a_n x^n + \cdots + a_0 \in k[x]$ be a separable polynomial of degree $n \geq 5$ and consider the plane affine curve C_0 defined by the equation

$$y^2 = f(x). \tag{2}$$

The curve C_0 is smooth and its closure $\tilde{C}$ in $\mathbb{P}^2$ has only one point at infinity, P_∞, which is always a singular point. The normalization $C \to \tilde{C}$ of $\tilde{C}$ is an hyperelliptic curve of genus $[n-1/2]$. If n is odd, the point P_∞ has only one preimage in C, which we still denote by P_∞; this point is a Weierstrass point and it is always defined over k. If n is even the point P_∞ has two preimages in C, which we denote by P_{∞_1}, P_{∞_2}; they are defined over k if and only if a_n is a square in k^*.

Since the rest of the points of C are in bijection with the points in C_0, it is common to attach to these points of C the affine coordinates (x, y) of the corresponding points in C_0. If we introduce affine coordinates in $\mathbb{P}^1$ (by declaring some point in $\mathbb{P}^1(k)$ to be ∞), the map

$$x : C_0 \to \mathbb{P}^1, \qquad (x, y) \mapsto x, \tag{3}$$

extends to a degree 2 map from C to $\mathbb{P}^1$ sending P_∞ or the pair $P_{\infty_1}, P_{\infty_1}$ to ∞. The Weierstrass points of C coincide with the ramification points of x. Every hyperelliptic curve of genus $g \geq 2$ defined over k is k-isomorphic to some curve C obtained as above. If k is algebraically closed, two hyperelliptic curves of genus g are k-isomorphic if and only if the images in $\mathbb{P}^1(k)$ of the $2g+2$ Weierstrass points under any degree 2 map from the curve to $\mathbb{P}^1$ differ by a k-automorphism of $\mathbb{P}^1$. For a non-algebraically closed field there are quadratic twists to deal with.

Given any $\lambda \in k^*/k^{*2}$ and a curve C given by Eq. (2) we define the twisted curve C^λ as the one determined by the equation

$$y^2 = \lambda f(x).$$

For a fixed positive integer $g \geq 2$ denote by $\mathscr{H}$ the set of k-isomorphy classes of hyperelliptic curves defined over k of genus g. The curves C and C^λ are isomorphic over the quadratic extension $k(\sqrt{\lambda})$, but they are not necessarily k-isomorphic. This induces a well-defined action of k^*/k^{*2} on $\mathscr{H}$ and we denote by $\mathscr{H}^t$ the quotient set $\mathscr{H}\backslash(k^*/k^{*2})$.

Denote by $\mathscr{X}$ the set of k-points of the variety $\binom{\mathbb{P}^1}{2g+2}$ of $2g+2$-subsets of $\mathbb{P}^1$. That is, the elements in $\mathscr{X}$ are families $\{x_1, \ldots, x_{2g+2}\}$ of $2g+2$ different points of $\mathbb{P}^1(\bar{k})$ invariant under the galois action:

$$\{x_1, \ldots, x_{2g+2}\} = \{x_1^\sigma, \ldots, x_{2g+2}^\sigma\}, \qquad \forall \sigma \in \mathrm{Gal}(\bar{k}/k).$$

The variety $\mathscr{M} = \binom{\mathbb{P}^1}{2g+2}\backslash \mathrm{PGL}_2$ is a coarse moduli space for hyperelliptic curves of genus g. Its sets of k-points is $\mathscr{M}(k) = \mathscr{X}\backslash \mathrm{PGL}_2(k)$.

Consider the map

$$W : \mathscr{H}^t \to \mathscr{M}(k), \tag{4}$$

which assigns to any curve C the class of the set $\{x(P_1), \ldots, x(P_{2g+2})\}$ of images of the Weierstrass points $P_1, \ldots, P_{2g+2}$ of C under any degree 2 map, $x : C \to \mathbb{P}^1$. This map W is well defined and bijective. The inverse map sends $\{x_1, \ldots, x_{2g+2}\}$ to the curve C defined by the equation

$$y^2 = \prod_{x_i \neq \infty} (x - x_i).$$

Therefore, if $k = \mathbb{F}_q$ is a finite field with odd characteristic, the formula of Theorem 2.2 for $n = 2g+2$ counts the number of hyperelliptic curves of genus g defined over k, up to k-isomorphism and quadratic twist.

In the table below we write down these numbers for $g = 2, 3, 4, 5$.

g	$\lvert\mathscr{H}^t\rvert$
2	$q^3 + q^2 + q + [4]_{q\equiv 1(5)} + [1]_{q\equiv 0(5)} + [-1]_{q\equiv 0(3)}$
3	$q^5 + q^3 - 1 + [q]_{q\not\equiv 0(3)} + [6]_{q\equiv 1(7)} + [1]_{q\equiv 0(7)} + [2]_{q\equiv \pm 1(8)}$
4	$q^7 + q^4 + [q^2 - q + 2]_{q\equiv 1(3)} - [q^2 - q]_{q\equiv -1(3)} + [q-1]_{q\equiv 0(5)} + [2q]_{q\equiv \pm 1(5)} + [6]_{q\equiv 1(9)} + [2]_{q\equiv \pm 1(8)}$
5	$q^9 + q^5 + 1 + [2q-2]_{q\equiv 1(3)} + [2q]_{q\equiv \pm 1(5)} + [10]_{q\equiv 1(11)} + [1]_{q\equiv 0(11)} + [-2]_{q\equiv -1(4)} + [2]_{q\equiv \pm 1(12)}$

Furthermore, it is clear that the set of $2g + 2$ Weierstrass points of an hyperelliptic curve C defined over k is galois invariant. The cardinals of the invariant subsets of this galois set furnish a partition of the positive integer $2g + 2$ and since all galois groups over a finite field are cyclic, this partition actually determines the structure of the galois set. Clearly, the structure of this galois set is invariant under isomorphism and under quadratic twist; thus, the set $\mathscr{H}^t$ is the disjoint union of $p(2g + 2)$ subsets, each one gathering classes of curves with the same galois structure of the set Weierstrass points. For instance, if $g = 2$ we have

$$\mathscr{H}^t = \mathscr{H}^t_{1,1,1,1,1,1} \cup \mathscr{H}^t_{2,1,1,1,1} \cup \mathscr{H}^t_{2,2,1,1} \cup \mathscr{H}^t_{2,2,2} \cup \mathscr{H}^t_{3,1,1,1} \cup$$

$$\mathscr{H}^t_{3,2,1} \cup \mathscr{H}^t_{3,3} \cup \mathscr{H}^t_{4,1,1} \cup \mathscr{H}^t_{4,2} \cup \mathscr{H}^t_{5,1} \cup \mathscr{H}^t_{6},$$

where, for instance, $\mathscr{H}^t_{4,1,1}$ denotes the set of classes of curves in $\mathscr{H}$ having two Weierstrass points defined over k and four Weierstrass points defined over the quartic extension of k, forming a complete orbit under the action of $\mathrm{Gal}(\bar{k}/k)$.

Exactly in the same way, the sets $\mathscr{X}$ and $\mathscr{M}(k) = \mathscr{X}\backslash\mathrm{PGL}_2(k)$ split as the union of $p(2g + 2)$ different subsets and the map W of (4) respects this decomposition. This is clearly seen if we consider the particular degree 2 map from C to $\mathbb{P}^1$ given in (3) for which the Weierstrass points have affine coordinates $(x, 0)$.

Corresponding to the partition $n = 1 + 1 + \cdots + 1$ we get the subset of $\mathscr{H}^t$ of classes, modulo k-isomorphism and quadratic twist, of hyperelliptic curves of genus g defined over k having all Weierstrass points defined over k, that is, hyperelliptic curves given by Eqs. (2) with a polynomial $f(x)$ having all its roots in k. By the above considerations, the map W gives a bijection between this set of classes of curves and the set of orbits of n-sets of $\mathbb{P}^1(k)$ under the action of $\mathrm{PGL}_2(k)$. In [5] a closed formula was obtained for this latter number of orbits.

More generally, it would be interesting to find explicit formulas for the cardinal of each subset of $\mathscr{X}\backslash\mathrm{PGL}_2(k)$ gathering classes of n sets with fixed structure as a galois set. In this way we would obtain, in the odd characteristic case, explicit formulas for the number of hyperelliptic curves defined over k, up to k-isomorphism and quadratic twist, with a fixed galois structure for the set of Weierstrass points. We hope to deal with this question elsewhere.

REFERENCES

1. A. Betten, H. Fripertinger, A. Kerber, A. Wassermann, and K.-H. Zimmermann, "Codierungstheorie," Springer-Verlag, New York/Berlin, 1998.
2. J. Cassels and E. Flynn, "Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2," Cambridge Univ. Press, Cambridge, UK, 1996.
3. J. Harris, "Algebraic Geometry, a First Course," Grad. Texts in Math., Vol. 133, Springer-Verlag, New York, 1992.
4. J. W. P. Hirschfeld, "Projective Geometries over Finite Fields," Clarendon, Oxford, 1979.
5. A. López and E. Nart, Classification of Goppa codes of genus zero, *J. Reine Angew. Math.* **517** (1999), 131–144.
6. A. J. Menezes, Y.-H. Wu, and R. J. Zuccherato, An elementary introduction to hyperelliptic curves, *in* "Algebraic Aspects of Cryptography," (N. Koblitz, Ed.), Springer-Verlag, New York/Berlin, 1999.
7. M. A. Tsfasman and S. G. Vlădut, "Algebraic-Geometric Codes," Kluwer Academic, Dordrecht, 1991.