DISSERTATION

COUNTING ARTIN-SCHREIER CURVES OVER FINITE FIELDS

Submitted by

Anne M. Ho

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Fall 2015

Doctoral Committee:

Advisor: Rachel Pries

Jeff Achter
Myung Hee Lee
Tim Penttila

Copyright by Anne M. Ho 2015

All Rights Reserved

ABSTRACT

COUNTING ARTIN-SCHREIER CURVES OVER FINITE FIELDS

Several authors have considered the weighted sum of various types of curves of a certain genus g over a finite field $k := \mathbb{F}_q$ of characteristic p where p is a prime and $q = p^m$ for some positive integer m. These include elliptic curves (Howe), hyperelliptic curves (Brock and Granville), supersingular curves when $p = 2$ and $g = 2$ (Van der Geer and Van der Vlught), and hyperelliptic curves of low genus when $p = 2$ (Cardona, Nart, Pujolàs, Sadornil). We denote this weighted sum

$$\sum_{[C]} \frac{1}{|\mathrm{Aut}_k(C)|},$$

where the sum is over k-isomorphism classes of the curves and $\mathrm{Aut}_k(C)$ is the automorphism group of C over k.

Many of these curves mentioned above are Artin-Schreier curves, so we focus on these in this dissertation. We consider Artin-Schreier curves C of genus $g = d(p-1)/2$ for $1 \leq d \leq 5$ over finite fields k of any characteristic p. We also determine a weighted sum for an arbitrary genus g in one-, two-, three-, and four-branch point cases. In our cases, we must consider a related weighted sum

$$\sum_{[C]} \frac{1}{|\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle|},$$

where $\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle$ is the centralizer of $\langle\iota\rangle$ in $\mathrm{Aut}_k(C)$. We discuss our methods of counting, our results, applications, as well as geometric connections to the moduli space of Artin-Schreier covers.

ACKNOWLEDGEMENTS

I would like to thank Rachel Pries for her guidance and my committee members for their research ideas throughout this process. I would also like to thank my family and C. for their support.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1

Introduction

Let $k = \mathbb{F}_q$ be a finite field of characteristic p, where p is a prime and $q = p^m$ for some positive integer m. An Artin-Schreier curve is a curve C for which there exists a degree p Galois cover $\pi : C \to \mathbb{P}^1$. The cover π corresponds to an extension of function fields

$$k(x) \hookrightarrow \frac{k(x)[y]}{(y^p - y - u(x))},$$

where $u(x)$ is a rational function. A generator of the Galois group is $\iota := (x, y) \mapsto (x, y+1)$, which has order p. The curve C has an associated rational equation $y^p - y = u(x)$, although this equation is not uniquely determined. The genus of an Artin-Schreier curve is a multiple of $(p-1)/2$. Let $\mathrm{Aut}_k(C)$ be automorphism group of C over k and $|\mathrm{Aut}_k(C)|$ be the order of the group.

Several authors have considered the weighted sum of curves of a given genus.

First, Everett Howe considered the genus one case [5, Corollary 2.2]. He proved that

$$\sum_{[C]} \frac{1}{|\mathrm{Aut}_k(C)|} = q \text{ for } g = 1,$$

where the sum is over all k-isomorphism classes of elliptic curves. Note when $p = 2$, then the elliptic curves are Artin-Schreier curves.

Bradley Brock and Andrew Granville considered hyperelliptic curves of genus g for odd primes p [1, Proposition 7.1], and the weighted sum is

$$\sum_{[C]} \frac{1}{|\mathrm{Aut}_k(C)|} = q^{2g-1} \text{ for odd } p, \text{ genus } g.$$

Gerard van der Geer and Marcel van der Vlugt looked at supersingular curves of genus two [3, Corollary 5.3]. Their result is that

$$\sum_{[C]} \frac{1}{|\mathrm{Aut}_k(C)|} = q \text{ for } p = 2, g = 2.$$

Gabriel Cardona, Enric Nart, and Jordi Pujolàs examined all Artin-Schreier curves of genus two over a finite field of characteristic two [2, Theorem 18]. They found the weighted sum for various subcases, including the supersingular case, which, when combined, gave the result that

$$\sum_{[C]} \frac{1}{|\mathrm{Aut}_k(C)|} = q^3 \text{ for } p = 2, g = 2.$$

Later, Enric Nart and Daniel Sadornil extended these results for Artin-Schreier curves of genus three over a finite field of characteristic two [10, Theorem 8]. The weighted sum here is

$$\sum_{[C]} \frac{1}{|\mathrm{Aut}_k(C)|} = q^5 \text{ for } p = 2, g = 3.$$

In all of these results, the authors have explicit formulas for subcases indexed by ramification data of π.

Following [2] and [10], we consider the weighted sum of Artin-Schreier curves of given genus g over a finite field of characteristic p. It turns out that the $p = 2$ case is easier because $\langle \iota \rangle$ is in the center of $\mathrm{Aut}_k(C)$ when $p = 2$, but this is not always true for odd p [4]. Thus, instead of weighting the count by the size of $\mathrm{Aut}_k(C)$, we consider a weighted count by the size of the centralizer of $\langle \iota \rangle$ in $\mathrm{Aut}_k(C)$ in all cases. We denote this by $\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle \iota \rangle$.

Specifically, our main results are the weighted sum for the cases in which the genus is $g = d(p-1)/2$ for $1 \leq d \leq 5$ for arbitrary p. We have also found the weighted sum for an arbitrarily large genus g when the number of branch points is at most four, and the number

of branch points is the number of poles in the rational equation $u(x)$. Details of the results are found in Chapter 3.

We use similar methods as in [2] and [10]. First, we start by dividing the situation into cases indexed by discrete information about the ramification divisor of π. We find the appropriate structure for the rational equations in each case. We count the total number of rational equations and then describe the conditions for two covers to be k-isomorphic. Next, we determine the size of the centralizer of $\langle \iota \rangle$ for each case by examining possible automorphisms γ of $\mathbb{P}^1$, which fix the discrete information about the ramification divisor. These automorphisms are contained in $\mathrm{PGL}_2(k)$, the projective general linear group, so we can view them as fractional linear transformations. These fractional linear transformations act on our rational equations $u(x)$. In addition, the generator ι of the Galois group of π also acts on the rational equations.

Finally, we add up the counts appropriately to get a weighted sum. We find that the one-, two-, and three-branch point cases are similar to each other, whereas the four-branch point cases are more complicated because they involve more complicated orbits of $\mathrm{PGL}_2(\overline{k})$ on four-sets of $\mathbb{P}^1(k)$. For these sets of four branch points, we use Burnside's Lemma to count the orbits.

In our cases, we also determine explicit formulas for the weighted counts of the Artin-Schreier curves.

For $p = 3, g = d(p-1)/2$, we have Theorem 4.2.4:

$$\sum_{[C]} \frac{1}{|\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle|} = \begin{cases} 1 & \text{if } g = 1 \\ q-1 & \text{if } g = 2 \\ q^2 & \text{if } g = 3 \\ 2q^3 - q^2 & \text{if } g = 4 \\ q^4 & \text{if } g = 5 \end{cases}$$

and for $p \geq 5, g = d(p-1)/2$, we have Theorem 4.2.6:

$$\sum_{[C]} \frac{1}{|\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle|} = \begin{cases} 1 & \text{if } g = 1(p-1)/2 \\ 2q-1 & \text{if } g = 2(p-1)/2 \\ 2q^2 - q & \text{if } g = 3(p-1)/2 \\ 3q^3 - 3q^2 & \text{if } g = 4(p-1)/2, p = 5 \\ 4q^3 - 3q^2 & \text{if } g = 4(p-1)/2, p \geq 7 \\ 3q^4 - 3q^3 + q^2 & \text{if } g = 5(p-1)/2, p = 5 \\ 4q^4 - 4q^3 + q^2 & \text{if } g = 5(p-1)/2, p \geq 7 \end{cases}$$

Our main counting theorems are found in Section 2.5.

Furthermore, we discuss the connection between our weighted sums and geometry in Section 4.2.1. It turns out that the coefficients from the weighted sums give information about the irreducible components of the moduli space for Artin-Schreier curves. In fact, the leading coefficient of the weighted sums corresponds to the number of components, and

the exponent of the leading term is the dimension. This explains the difference between the $p = 5$ and $p \geq 7$ cases.

CHAPTER 2

Weighted Number of Artin-Schreier Curves

2.1. Background

Let $k = \mathbb{F}_q$ be a finite field of characteristic p, where p is a prime and $q = p^m$ for some positive integer m. Let $\bar{k}$ be an algebraic closure of k. We consider C, a smooth, projective, geometrically irreducible curve defined over k.

The following is a summary of Artin-Schreier covers from [12]. An Artin-Schreier curve C is a curve for which there is a degree p Galois cover $\pi : C \to \mathbb{P}^1$. C has an associated rational equation $y^p - y = u(x) \in k(x)$. In this case, the cover corresponds to an extension of function fields,

$$k(x) \hookrightarrow \frac{k(x)[y]}{(y^p - y - u(x))},$$

which is a cyclic extension of degree p. A generator of the Galois group is $\iota := (x, y) \mapsto (x, y + 1)$, which has order p.

Theorem 2.1.1. *[9, Proposition 3.4.12] The fixed points of ι are the ramification points of the degree p map $\pi : C \to \mathbb{P}^1$.*

The hyperelliptic covers of [2] and [10] are in the case when $p = 2$, and this ι is the hyperelliptic involution mentioned in their papers.

Let $\mathrm{Aut}_k(C)$ denote the automorphism group of C over k. We consider the weighted sum

$$\sum_{[C]} \frac{1}{|\mathrm{Aut}_k(C)|}$$

where $[C]$ ranges over the k-isomorphism classes of C. If we want to consider the entire automorphism group of C over k though, we find that it is elusive in some exceptional cases:

THEOREM 2.1.2. *[4, 11.93]*

(1) If $p = 2$, then $\langle \iota \rangle$ is in the center of $\mathrm{Aut}_k(C)$.

(2) If p is odd, then $\langle \iota \rangle$ is normal in $\mathrm{Aut}_k(C)$ except in these cases with the following rational equations:

(a) $y^p - y = a/(x^p - x)$ for $a \in k$,

(b) $y^3 - y = b/x(x-1)$ with $b^2 = 2$, or

(c) $y^p - y = 1/x^c$ with $c \mid (p+1)$.

This means that to include all primes p for our results, we will use the centralizer of $\langle \iota \rangle$ in the automorphism group of C instead of the automorphism group itself. We denote the centralizer as $\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle \iota \rangle$. This allows us to finish the case for genus $g = d(p-1)/2$ for $1 \leq d \leq 5$.

To count Artin-Schreier curves, we first divide our various cases into subcases. Given a genus g, we look at the structure of the ramification divisor and the splitting behavior, which entails determining the possible structures of the fields of definitions of the poles in our rational equation $y^p - y = u(x)$. We can then fix a subcase and choose the locations of the poles. This allows us to write down a rational equation and count the number of rational equations. Finally, we find possible changes of variables for $y^p - y = u(x)$ and determine which subgroups of $\mathrm{PGL}_2(k)$, the projective general linear group, act on the representative equations for the Artin-Schreier covers.

2.2. Ramification Data and Splitting Behavior

2.2.1. Ramification Data. To count Artin-Schreier curves over finite fields of characteristic p up to k-isomorphism, we consider the rational equation for each cover defined over k based on the possible ramification divisors. We denote the ramification divisor of

π as $\mathrm{Diff}(C/\mathbb{P}^1)$. The ramification divisor is associated to the different of the extension of function fields mentioned above. We can consider the branch divisors W of $\mathbb{P}^1$, which are the push-forward of the ramification divisors of the Artin-Schreier covers. The set of multiplicities of the points in the branch divisor is a discrete invariant. The orders of the pole of $u(x)$ at a point is one less than the multiplicity of the point.

We only need to consider rational equations with no poles of order congruent to zero modulo p when working with a field of characteristic p because we can apply a change of coordinates replacing y by $y+c$ to modify $u(x)$ such that p does not divide the order of any pole.

Now define the Artin-Schreier group as follows:

$$\mathrm{AS}(k(x)) := \{u(x)^p - u(x) \mid u(x) \in k(x)\}.$$

Given $u(x) \in k(x)$, a cover C with equation $y^p - y = u(x)$ is irreducible if and only if $u(x) \notin \mathrm{AS}(k(x))$.

THEOREM 2.2.2. *[12, Proposition 3.7.8] Let $u(x) \in k(x) - \mathrm{AS}(k(x))$ be a rational function with no poles of order of a multiple of p. Let $C = C_{u(x)}$ be the Artin-Schreier cover defined over k, with equation $y^p - y = u(x)$, and let $P \in C(\bar{k})$. Then*

$$\mathrm{Diff}(C/\mathbb{P}^1) = \sum_{Q \in \mathbb{P}^1(\bar{k})} \left(\sum_{P \mapsto Q} (\epsilon_Q + 1)P \right)$$

where

$$\epsilon_Q = \begin{cases} -1 & \text{if } \mathrm{ord}_Q(u(x)) \geq 0 \\ m & \text{if } \mathrm{ord}_Q(u(x)) = -m < 0 \end{cases}$$

Here, we have that

$$\deg(\mathrm{Diff}(C/\mathbb{P}^1)) = \sum_{Q\in\beta}(\epsilon_Q + 1)(p-1)$$

where $\beta = \{Q_i\}$ *is the branch locus. Furthermore,*

$$k(C) \cap \bar{k} = k \Leftrightarrow u(x) \notin k + \mathrm{AS}(k(x)) \Leftrightarrow \mathrm{Diff}(C/\mathbb{P}^1) \neq 0.$$

When this condition is satisfied, $\deg(\mathrm{Diff}(C/\mathbb{P}^1)) = 2g + 2(p-1)$*, where* g *is the genus of* C*.*

Here, the genus means the dimension of the vector space of regular 1-forms.

In essence, given a genus g and a prime p, we have a number that is $\deg(\mathrm{Diff}(C/\mathbb{P}^1))$. To determine the ramification possibilities, we consider the partitions of $\deg(\mathrm{Diff}(C/\mathbb{P}^1))/(p-1)$ into numbers not congruent to 1 mod p. For instance, if $g = 2(p-1)$ and p is any prime greater than 5, then $\deg(\mathrm{Diff}(C/\mathbb{P}^1))/(p-1) = 6$, so possible partitions are (6), (4,2), (3,3), and (2,2,2).

2.2.3. Splitting Behavior. For the different ramification types, there are different possibilities of whether the poles of $u(x)$ are defined over k or over a larger field $\mathbb{F}_{q^m}$. These give various splitting types. For the cases that we consider in which we have one to four branch points, we call these the split, split+quadratic, quadratic, cubic, and quartic cases, indicating that the branch points are all defined over k, that two are defined over $\mathbb{F}_{q^2}\backslash\mathbb{F}_q$, that two pairs are defined over $\mathbb{F}_{q^2}\backslash\mathbb{F}_q$, that three are defined over $\mathbb{F}_{q^3}\backslash\mathbb{F}_q$, or that four are defined over $\mathbb{F}_{q^4}\backslash\mathbb{F}_{q^2}$.

The associated rational equation $y^p - y = u(x)$ must be defined over k, but the poles of $u(x)$ do not have to be in k necessarily. We can write a partial fraction decomposition of $u(x)$ over $\overline{k}$.

First, we introduce the Frobenius endomorphism, $\mathrm{Fr} : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$, where $\mathrm{Fr}(\alpha) = \alpha^q$. In other words, this is the qth power map.

LEMMA 2.2.4. *Let $u(x) \in \mathbb{F}_q(x)$ be such that $\mathrm{div}_\infty(u(x)) = \epsilon b$, where b is an $\mathbb{F}_q$-point of degree m and $\epsilon \in \mathbb{N}$. Let* Fr *be the Frobenius endomorphism. Then there exist $c_0 \in \mathbb{F}_q$ and $v(x) \in \mathbb{F}_{q^m}(x)$ such that $\mathrm{div}_\infty(v(x)) = \epsilon b_1$ for some $\mathbb{F}_{q^m}$-point b_1 of degree one and*

$$u(x) = \sum_{j=1}^{m-1} \mathrm{Fr}^j(v(x)) + c_0.$$

PROOF. Let $u(x) \in \mathbb{F}_q(x)$ be such that $\mathrm{div}_\infty(u(x)) = \epsilon b$. The $\mathbb{F}_q$-point b is an orbit $\{\theta_1, \theta_2, \cdots, \theta_m\}$ of $\mathbb{F}_{q^m}$-points θ_i under the Frobenius map. If we consider the partial fraction decomposition of $u(x) \in \mathbb{F}_{q^m}(x)$, then

$$u(x) = \sum_{j=0}^{m-1} \frac{v_j(x)}{(x - \theta_j)^\epsilon} + c_0$$

where $v_j(x) \in \mathbb{F}_{q^m}[x]$ is a polynomial of degree $\epsilon - 1$ with nonzero constant term. Apply the Frobenius map to both sides to obtain

$$\mathrm{Fr}(u(x)) = \sum_{j=0}^{m-1} \frac{\mathrm{Fr}(v_j(x))}{(x - \theta_{j+1})^\epsilon} + \mathrm{Fr}(c_0)$$

where $\theta_m = \theta_0$. Since $\mathrm{Fr}(u(x)) = u(x)$, $v_j(x) = \mathrm{Fr}(v_{j-1}(x))$, and $\mathrm{Fr}(c_0) = c_0$, then

$$u(x) = \sum_{j=0}^{m-1} \mathrm{Fr}^j \left(\frac{v_1(x)}{(x - \theta_1)^\epsilon} \right) + c_0.$$

□

In other words, if the branch points are not defined over k, the condition that $u(x) \in k(x)$ places constraints on the partial fraction decomposition. In particular, terms in the partial fraction decomposition must respect the action of the Frobenius map.

Explicitly, for a given ramification type and splitting type that corresponds to having four branch points $\theta_1, \theta_2, \theta_3$, and θ_4 defined over k of orders $\epsilon_1, \epsilon_2, \epsilon_3$, and ϵ_4, respectively, the partial fraction decomposition of $u(x)$ looks like:

$$\begin{aligned} y^p - y &= \frac{c_{1,1}x^{\epsilon_1-1} + \cdots + c_{1,i}x^{\epsilon_1-i} + \cdots + c_{1,\epsilon_1}}{(x-\theta_1)^{\epsilon_1}} + \frac{c_{2,1}x^{\epsilon_2-1} + \cdots + c_{2,j}x^{\epsilon_2-j} + \cdots + c_{2,\epsilon_2}}{(x-\theta_2)^{\epsilon_2}} \\ &+ \frac{c_{3,1}x^{\epsilon_3-1} + \cdots + c_{3,l}x^{\epsilon_3-l} + \cdots + c_{3,\epsilon_3}}{(x-\theta_3)^{\epsilon_3}} + \frac{c_{4,1}x^{\epsilon_4-1} + \cdots + c_{4,n}x^{\epsilon_4-n} + \cdots + c_{4,\epsilon_4}}{(x-\theta_4)^{\epsilon_4}} + c_0 \end{aligned}$$

where $1 < i < \epsilon_1, 1 < j < \epsilon_2, 1 < l < \epsilon_3$, and $1 < n < \epsilon_4$.

2.3. Rational Equations

Now we can fix a subcase and choose the locations of the poles for our rational equation.

To count Artin-Schreier curves over k for a fixed genus g, we first choose the number of branch points. From here, we can choose the splitting type and then the branch divisor W. Since the divisor W is defined over k, then supposing we have four branch points, we could have the following possibilities:

TABLE 2.1. Fields of Definitions for Poles

Splitting Type	Poles	Field of Definition
Split	$\infty, 0, 1, t$ for $t \in k \backslash \{0, 1\}$	k
Split + Quadratic	$\infty, 0, \theta, \theta'$	$\infty, 0 \in k$; $\theta, \theta' \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$
Quadratic	$\theta, \theta', \tau, \tau'$	$\mathbb{F}_{q^2} \backslash \mathbb{F}_q$
Cubic	$\infty, \theta, \theta', \theta''$	$\infty \in k; \theta, \theta', \theta'' \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$
Quartic	$\theta, \theta', \theta'', \theta'''$	$\theta, \theta', \theta'', \theta''' \in \mathbb{F}_{q^4} \backslash \mathbb{F}_{q^2}$

When we have fewer branch points, we have a subset of these various splitting types.

We can count the coefficients for each term in the partial fraction decomposition as follows:

LEMMA 2.3.1. *(1) Consider the set*

$$S = \{u(x) \in x\mathbb{F}_{q^r}[x] \mid \deg u(x) = \epsilon\}$$

where $u(x)$ has no exponents of degree $0 \bmod p$. The cardinality of S is $(q^r - 1)q^{r\left(\epsilon - 1 - \lfloor \frac{\epsilon}{p} \rfloor\right)}$.

(2) Let P be a point defined over $\mathbb{F}_{q^r}$ in which $\mathrm{div}_\infty(u(x)) = \epsilon P$. Then, the number of representative equations up to Artin-Schreier equivalence is $(q^r - 1)q^{r\left(\epsilon - 1 - \lfloor \frac{\epsilon}{p} \rfloor\right)}$.

PROOF. (1) First, we can write $u(x)$ as

$$u(x) = \sum_{j=0}^{\epsilon} c_j x^j$$

where c_j are coefficients in $\mathbb{F}_{q^r}$. Since $u(x)$ must be of degree ϵ, there are $q^r - 1$ choices for c_ϵ and q^r choices for the rest of the coefficients. There are only terms in which $j \neq 0 \bmod p$, so there are $\epsilon - 1 - \lfloor \frac{\epsilon}{p} \rfloor$ such choices.

(2) If P is the point at infinity, then let x be as is from part (1). If P is $\theta_r \in \mathbb{F}_{q^r}$, then let $x = 1/(x - \theta_r)$, and the statement follows from part (1).

□

In addition, for the rational equation of an Artin-Schreier cover, we have a constant term $c_0 \in k$. For any $u(x)$ and $u'(x)$, the Artin-Schreier covers $C_{u(x)}$ and $C_{u'(x)}$ are k-isomorphic if there exists $\gamma \in \mathrm{PGL}_2(k)$ such that $u'(x) \equiv \gamma(u(x)) \bmod \mathrm{AS}(k(x))$.

LEMMA 2.3.2. *Let* $\mathrm{AS}(k) = \{r^p - r \mid r \in k\} \subset k$. *There are* q/p *elements in* $\mathrm{AS}(k)$.

PROOF. Take the map $\varphi : k \to k$ defined by $r \mapsto r^p - r$. This is a homomorphism of additive groups because for $r_1, r_2 \in k$,

$$\begin{aligned} \varphi(r_1 + r_2) &= (r_1 + r_2)^p - (r_1 + r_2) \\ &= r_1^p + r_2^p - r_1 - r_2 \\ &= (r_1^p - r_1) + (r_2^p - r_2) \\ &= \varphi(r_1) + \varphi(r_2). \end{aligned}$$

Consider the kernel of φ:

$$\begin{aligned} \ker(\varphi) &= \{r \in k \mid r^p - r = 0\} \\ &= \{r \in k \mid r^p = r\} \\ &= \{r \mid r \in \mathbb{F}_p\} \end{aligned}$$

indicating that $|\ker(\varphi)| = p$.

In addition, the image of φ is $\mathrm{AS}(k)$. There are q elements in k, so

$$|\mathrm{AS}(k)| = |\mathrm{Im}(\varphi)| = q/p.$$

□

Corollary 2.3.3. *For a fixed $v(x) \in k(x)$ and for $c_0 \in k$, let $C_{c_0} : y^p - y = v(x) + c_0$. The number of isomorphism classes of $\{C_{c_0} \mid c_0 \in k\}$ is p.*

Proof. Two such covers C_{c_0} and $C_{c_0'}$ are isomorphic if and only if $c_0 - c_0' = r^p - r$ for some $r \in k$, in other words, they are isomorphic if and only if $c_0 - c_0' = \mathrm{AS}(k)$. The number of isomorphism classes equals the number of cosets of $\mathrm{AS}(k)$ in k, which is p. □

Thus, the number of choices for the constant term of our rational equation is p.

2.4. Group Actions

Before we prove our main counting theorem, we first introduce some notation:

Symbol	Denotes
R	ramification type
S	splitting type
W	branch divisor
$\mathcal{N} = \mathcal{N}_{R,S}$	$\{y^p - y = u(x) \mid \mathrm{div}_\infty(u(x))$ is of type $R, S\}$
$\mathcal{N}_W$	$\{y^p - y = u(x) \in \mathcal{N} \mid u(x)$ has branch divisor $W\}$
Γ_W	$\{\gamma \in \mathrm{PGL}_2(k) \mid \gamma(W) = W\}$
$\Gamma_{u(x)}$	$\{\gamma \in \Gamma_W \mid u(x) = u(\gamma(x))\}$

Note that in the split case with four branch points, $\mathcal{N}$, $\mathcal{N}_W$, Γ_W, and $\Gamma_{u(x)}$ depend on the choice of a fourth branch point $t \in k\backslash\{0,1\}$, so we will denote these with an additional subscript t. Furthermore, if there are more than three branch points, say n, we have:

Symbol	Denotes
θ	set of orbits of n-sets in $\mathbb{P}^1(\overline{k})$ under $\mathrm{PGL}_2(k)$
θ_H	set of orbits of n-sets in which Γ_W is conjugate to H for $H \subset S_n$

There is the problem that the same cover can be written down with different rational equations, so we need to know when two covers are isomorphic. Let $\gamma \in \mathrm{PGL}_2(k)$ be the possible automorphisms of $\mathbb{P}^1$ and $\Gamma_W := \{\gamma \mid \gamma \in \mathrm{PGL}_2(k), \gamma(W) = W\}$. In other words, Γ_W is the stabilizer of the branch locus.

Note that elements $\gamma \in \mathrm{PGL}_2(k)$ can be seen as fractional linear transformations

$$\gamma(x) = \frac{ax+b}{cx+d}. \tag{1}$$

We will use this rational equation to describe Γ_W in more detail for each case of our results. We can also view these mappings as 2×2 matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with nonzero determinant for $a, b, c, d \in k$. Two matrices M and M' are equivalent if $M' = \lambda M$ for $\lambda \in k$.

Along with the aforementioned $\gamma \in \mathrm{PGL}_2(k)$, there is ι from Section 2.1, which is an automorphism written as $\iota : (x, y) \mapsto (x, y+1)$ in affine coordinates.

DEFINITION 2.4.1. *Let $\pi_1 : C_1 \to \mathbb{P}^1$ and $\pi_2 : C_2 \to \mathbb{P}^1$ be two Artin-Schreier covers. We say that an isomorphism of covers $\varphi : C_1 \to C_2$ exists if and only if there exists $\gamma \in \mathrm{Aut}(\mathbb{P}^1)$ such that the following diagram commutes:*

$$\begin{array}{ccc} C_1 & \xrightarrow{\varphi} & C_2 \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{P}^1 & \xrightarrow{\gamma} & \mathbb{P}^1 \end{array}$$

Equivalently, if C_1 is associated to $y^p - y = u_1(x)$ and C_2 is associated to $y^p - y = u_2(x)$, then the two covers are isomorphic if and only if there exists $\gamma \in \mathrm{Aut}(\mathbb{P}^1)$ such that $\gamma(u_1(x)) = u_2(x)$.

Note that if two covers are k-isomorphic, then they have the same ramification type R and splitting type S. Furthermore, the size of the stabilizer Γ_W is the same.

Now that we know when two covers are isomorphic, we can count the number of covers. Note that Γ_W acts on the set of representatives $\mathcal{N}_W$ for the rational functions $u(x) \in k(x)$, which we determine by counting the coefficients for a typical rational function given the ramification type. The number of isomorphism classes is the number of orbits.

THEOREM 2.4.2. *Suppose φ is an element of $\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle$.*

(1) There exists a mapping $\gamma : \mathbb{P}^1 \to \mathbb{P}^1$ such that $\pi \circ \varphi = \gamma \circ \pi$, where $\pi : C \to \mathbb{P}^1$.

(2) The map $\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle \to \mathrm{Aut}_k\mathbb{P}^1$ is a homomorphism and there is an exact sequence of groups:

$$1 \to \langle\iota\rangle \xrightarrow{I} \mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle \xrightarrow{\psi} \mathrm{Aut}(\mathbb{P}^1).$$

(3) Furthermore, $\mathrm{Im}(\psi) = \Gamma_{u(x)}$.

PROOF. Given a point $x \in \mathbb{P}^1$ and a $y \in C$ such that $\pi(y) = x$, we define $\gamma(x) = \pi(\varphi(y))$.

We show that this is well-defined. Suppose that $\pi(y_1) = \pi(y_2) = x$ for $y_1, y_2 \in C$. Then

$$y_2 = \iota^e(y_1)$$

for some power e of ι. Applying φ, we get

$$\begin{aligned} \varphi(y_2) &= \varphi(\iota^e(y_1)) \\ &= \iota^e(\varphi(y_1)) \end{aligned}$$

Both $\varphi(y_1)$ and $\varphi(y_2)$ are in $\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle$, so they are in the same orbit under $\langle\iota\rangle$. Thus, the fibers of π are these orbits, and

$$\pi(\varphi(y_1)) = \pi(\varphi(y_2)).$$

To show that γ is an automorphism, we note that γ is bijective because φ is bijective.

Next, consider the following diagram:

$$\begin{array}{ccccc} C & \xrightarrow{\varphi_1} & C & \xrightarrow{\varphi_2} & C \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{P}^1 & \xrightarrow{\gamma_1} & \mathbb{P}^1 & \xrightarrow{\gamma_2} & \mathbb{P}^1 \end{array}$$

Note that

$$\begin{aligned} (\gamma_2 \circ \gamma_1)(x) &= \pi(\varphi_2(\varphi_1(x))) \\ &= \pi(\varphi_2(y)) \circ \pi(\varphi_1(y)) \\ &= \gamma_2 \circ \gamma_1 \end{aligned}$$

In addition, we show that the sequence is exact. We show that the kernel $\ker(\psi) = \langle\iota\rangle$. Let $\psi(\iota) = \bar{\iota}$, then we have

$$\begin{aligned} \bar{\iota}(x) &= \psi(\iota(y_1)) \\ &= \psi(y_2) \\ &= x \end{aligned}$$

for some y_1 and y_2 which are in the same orbit under $\langle\iota\rangle$. Thus, $\bar{\iota}$ is the identity map and $\langle\iota\rangle \subseteq \ker(\pi)$.

On the other hand, suppose $\varphi \in \ker(\psi)$. The corresponding function field is

$$k(x) \hookrightarrow \frac{k(x)[y]}{(y^p - y - u(x))},$$

so $\varphi \in \ker(\psi)$ implies that $\varphi(x) = x$, meaning that $\varphi(u(x)) = u(x)$. Just consider $\varphi(y^p - y)$ then, which is $\varphi(y) = y + e$ for some number e, or that $\varphi(y) = \iota^e$. Thus, $\ker(\psi) \subseteq \langle\iota\rangle$, and $\ker(\psi) = \langle\iota\rangle$, meaning that the sequence is exact.

Lastly, we show that the image of ψ is equal to $\Gamma_{u(x)}$. Suppose $\overline{\gamma} \in \mathrm{Im}(\psi)$. This means that there exists a $\gamma : C_{u(x)} \to C_{u(x)}$ in which $u(\gamma(x)) = u(x)$, so $\mathrm{Im}(\psi) \subset \Gamma_{u(x)}$. Now if $\overline{\gamma} \in \Gamma_{u(x)}$, we can use this $\overline{\gamma}$ to define a $\gamma : C \to C$ in which $(x, y) \mapsto (\gamma(x), y)$. Since $\gamma \in \mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle$, then $\overline{\gamma} = \psi(\gamma)$ so $\Gamma_{u(x)} \subset \mathrm{Im}(\psi)$. □

From the short exact sequence in Theorem 2.4.2, we get that

$$|\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle| = p|\Gamma_{u(x)}|.$$

In addition, since Γ_W acts on $\mathcal{N}_W$, then an application of the Orbit-Stabilizer theorem results in

$$|\mathrm{Orb}_{\Gamma_W}(u(x))||\Gamma_{u(x)}| = |\Gamma_W|.$$

2.5. Main Theorems

We consider the weighted count that was originally studied by Gerard Van der Geer and Marcel Van der Vlugt in [3, Corollary 5.3].

Theorem 2.5.1. *Consider the branch divisor W and the set $\mathcal{N}_W = \{y^p - y = u(x)\}$ where $u(x)$ is a rational function with poles at W. We fix the ramification type R and the splitting type S of $u(x)$. Let Γ_W be the set of $\gamma \in \mathrm{PGL}_2(k)$ in which $\gamma(W) = W$. For three or fewer branch points, as $[C]$ ranges over the k-isomorphism classes of Artin-Schreier covers C of genus g, then*

$$\sum_{[C]} \frac{1}{|\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle|} = \frac{|\mathcal{N}_W|}{p|\Gamma_W|}.$$

Proof. We have

$$\sum_{[C]} \frac{1}{|\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle|} = \sum_{u(x)} \frac{1}{|\mathrm{Orb}_{\Gamma_W}(u(x))| \cdot p|\Gamma_{u(x)}|}$$

by changing the sum to be over all possible $u(x)$ and by the short exact sequence in Theorem 2.4.2. We divide by $|\mathrm{Orb}_{\Gamma_W}(u(x))|$ since the original sum was over k-isomorphism classes, and now we consider all $u(x)$, some of which represent the same isomorphism class. This equals

$$\sum_{u(x)} \frac{1}{p|\Gamma_W|}$$

by the Orbit-Stabilizer Theorem. Finally, this equals

$$\frac{|\mathcal{N}_W|}{p|\Gamma_W|}$$

since summing up 1 over all possible $u(x)$ is precisely the size of $\mathcal{N}_W$. □

THEOREM 2.5.2. *Consider the branch divisor W and the set $\mathcal{N}_W = \{y^p - y = u(x)\}$ where $u(x)$ is a rational function with poles at W. We fix the ramification type R and the splitting type S of $u(x)$. For $n \geq 4$ branch points, as $[C]$ ranges over the k-isomorphism classes of Artin-Schreier covers C of genus g defined over k, then*

$$\sum_{[C]} \frac{1}{|\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle|} = \frac{|\mathcal{N}_W|}{p} \sum_H \frac{|\theta_H|}{|H|}$$

where H ranges over conjugacy classes of subgroups of S_n, and θ_H is the set of orbits for the branch locus W in which Γ_W is conjugate to H.

PROOF. Let θ be the set of orbits of n-sets W in $\mathbb{P}^1(\overline{k})$ under $\mathrm{PGL}_2(k)$. We have

$$\sum_{[C]} \frac{1}{|\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle|} = \sum_{W\in\theta} \sum_{u(x)} \frac{1}{|\mathrm{Orb}_{\Gamma_W}(u(x))| \cdot p|\Gamma_{u(x)}|}$$

by changing the sum to be over all possible $u(x)$ and by the short exact sequence in Theorem 2.4.2. We divide by $|\mathrm{Orb}_{\Gamma_W}(u(x))|$ since the original sum was over k-isomorphism classes, and now we consider all $u(x)$, some of which represent the same isomorphism class. This double sum equals

$$\frac{1}{p} \sum_{W\in\theta} \sum_{u(x)} \frac{1}{|\Gamma_W|}$$

by the Orbit-Stabilizer Theorem. We rearrange the sums to be over the sets of orbits of n-sets in which Γ_W is conjugate to H for $H \subset S_n$, and we obtain

$$\frac{1}{p} \sum_{H} \sum_{\theta_H} \frac{1}{|H|} \sum_{u(x)} 1.$$

Since summing 1 over all possible $u(x)$ results in the size of $\mathcal{N}_W$, then we have

$$\frac{1}{p} \sum_{H} \sum_{\theta_H} \frac{|\mathcal{N}_W|}{|H|}.$$

Lastly, we pull $|\mathcal{N}_W|$ outside of the sum and have

$$\frac{|\mathcal{N}_W|}{p} \sum_{H} \sum_{\theta_H} \frac{1}{|H|} = \frac{|\mathcal{N}_W|}{p} \sum_{H} \frac{|\theta_H|}{|H|}$$

since the sum of 1 over θ_H is just $|\theta_H|$.

□

CHAPTER 3

Results on Weighted Sums

Let p be an arbitrary prime. Given the ramification divisor $\vec{\epsilon} := (\epsilon_1, \epsilon_2, \cdots, \epsilon_r)$, let

$$E := E(\vec{\epsilon}) = \sum_{i \geq 1} \left(\epsilon_i - 1 - \left\lfloor \frac{\epsilon_i}{p} \right\rfloor \right)$$

where p does not divide any ϵ_i.

3.1. Arbitrary Prime p, One, Two, and Three Branch Points

Proposition 3.1.1. *The following gives the weighted number of Artin-Schreier covers up to k-isomorphism:*

$$\sum_{[C]} \frac{1}{|\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle \iota \rangle|} =$$

Ramification Divisor	*Weighted Number of Covers*
(ϵ)	q^{E-1}
(ϵ_1, ϵ_2) *split*	$(q-1)q^E/s$ *where* $s = \begin{cases} 1 & \text{if } \epsilon_1 \neq \epsilon_2 \\ 2 & \text{if } \epsilon_1 = \epsilon_2 \end{cases}$
(ϵ, ϵ) *quadratic*	$(q-1)q^E/2$
$(\epsilon_1, \epsilon_2, \epsilon_3)$ *split*	$(q-1)^3q^E/s$ *where* $s = \begin{cases} 1 & \text{if } \epsilon_1, \epsilon_2, \epsilon_3 \text{ distinct} \\ 2 & \text{if } \epsilon_1 \neq \epsilon_2 = \epsilon_3 \\ 6 & \text{if } \epsilon_1 = \epsilon_2 = \epsilon_3 \end{cases}$
$(\epsilon_1, \epsilon_2, \epsilon_2)$ *quadratic*	$(q-1)(q^2-1)q^E/2$ *if* $\epsilon_1 \neq \epsilon_2$ *or* $\epsilon_1 = \epsilon_2$
$(\epsilon, \epsilon, \epsilon)$ *cubic*	$(q^3-1)q^E/3$

PROOF. The proofs for the one-, two-, and three-branch point cases are similar. Since the action of $\mathrm{PGL}_2(k)$ is triply transitive, we can fix the branch locus depending on the ramification divisor. Using Theorem 2.5.1, the weighted sum equals

$$\frac{|\mathcal{N}_W|}{p|\Gamma_W|}$$

where $|\mathcal{N}_W|$ is the number of rational functions $u(x)$ branched at W having poles of orders $\vec{\epsilon}$, and Γ_W is the subset of $\mathrm{PGL}_2(k)$ fixing W. The results follow once we verify the following table.

TABLE 3.1. $|\mathcal{N}_W|$ and $|\Gamma_W|$ for 1-,2-,3-Branch Point Cases

Case	$\lvert\mathcal{N}_W\rvert$	$\lvert\Gamma_W\rvert$
(ϵ)	$p(q-1)q^{E(\epsilon)}$	$q(q-1)$
(ϵ_1,ϵ_2) split	$p(q-1)^2q^{E(\epsilon_1,\epsilon_2)}$	$q-1$
(ϵ,ϵ) split	$p(q-1)^2q^{E(\epsilon,\epsilon)}$	$2(q-1)$
(ϵ,ϵ) quadratic	$p(q^2-1)q^{E(\epsilon,\epsilon)}$	$2(q+1)$
$(\epsilon_1,\epsilon_2,\epsilon_3)$ split	$p(q-1)^3q^{E(\epsilon_1,\epsilon_2,\epsilon_3)}$	1
$(\epsilon_1,\epsilon_2,\epsilon_2)$ split	$p(q-1)^3q^{E(\epsilon_1,\epsilon_2,\epsilon_2)}$	2
$(\epsilon,\epsilon,\epsilon)$ split	$p(q-1)^3q^{E(\epsilon,\epsilon,\epsilon)}$	6
$(\epsilon_1,\epsilon_2,\epsilon_2)$ or $(\epsilon,\epsilon,\epsilon)$ quadratic	$p(q-1)(q^2-1)q^{E(\epsilon_1,\epsilon_2,\epsilon_2)}$	2
$(\epsilon,\epsilon,\epsilon)$ cubic	$p(q^3-1)q^{E(\epsilon,\epsilon,\epsilon)}$	3

We can find $|\mathcal{N}_W|$ by using Lemma 2.3.1, which allows us to write a partial fraction decomposition of $u(x)$ and count coefficients, and Corollary 2.3.3, which gives the number of choices for the constant term.

Details for determining $|\Gamma_W|$ follow below. In the split cases, we choose our branch points W to be a subset of $\{\infty, 0, 1\}$, and we have:

TABLE 3.2. Γ_W for 1-,2-,3-Branch Point Cases

Case	Conditions	Γ_W
(ϵ)	$\gamma(\infty) = \infty$	$\{x \mapsto ax + b \mid a \in k^*, b \in k\}$
$(\epsilon_1, \epsilon_2), \epsilon_1 \neq \epsilon_2$	$\gamma(\infty) = \infty, \gamma(0) = 0$	$\{x \mapsto ax \mid a \in k^*\}$
(ϵ, ϵ)	$\gamma(\infty) = \infty, \gamma(0) = 0$	$\{x \mapsto ax \mid a \in k^*\}$, or
	$\gamma(\infty) = 0, \gamma(0) = \infty$	$\{x \mapsto 1/cx \mid c \in k^*\}$
$(\epsilon_1, \epsilon_2, \epsilon_3), \epsilon_1, \epsilon_2, \epsilon_3$ distinct	$\gamma(\infty) = \infty, \gamma(0) = 0, \gamma(1) = 1,$	$\{x \mapsto x\}$
$(\epsilon_1, \epsilon_2, \epsilon_2), \epsilon_1 \neq \epsilon_2$	$\gamma(\infty) = \infty, \gamma(0) = 0, \gamma(1) = 1,$	$\{x \mapsto x\}$, or
	$\gamma(\infty) = 0, \gamma(0) = \infty, \gamma(1) = 1$	$\{x \mapsto 1/x\}$
$(\epsilon, \epsilon, \epsilon)$	$\{\infty, 0, 1\} \mapsto \{\infty, 0, 1\}$	$\cong S_3$

In the non-split cases, note that $\mathrm{PGL}_2(k)$ acts transitively on the sets of degree two and degree three points, and $|\mathrm{PGL}_2(k)| = q(q+1)(q-1)$.

For the (ϵ, ϵ) quadratic case, we choose $W = \{\theta, \theta'\}$. There are $(q^2 - q)/2$ such pairs, so by the Orbit-Stabilizer Theorem,

$$|\Gamma_W| = \frac{|\mathrm{PGL}_2(k)|}{(q^2 - q)/2} = 2(q+1).$$

For the $(\epsilon_1, \epsilon_2, \epsilon_2)$ quadratic case in which $\epsilon_1 \neq \epsilon_2$ or $(\epsilon, \epsilon, \epsilon)$ quadratic case, we choose $W = \{\infty, \theta, \theta'\}$. Consider $\gamma \in \Gamma_W$ which are of the form in Equation 1. We must have $\gamma(\infty) = \infty$, which implies $c = 0$. For θ and θ', we consider maps of the pair to another pair.

We still have maps of the form

$$\gamma(x) = \frac{ax+b}{d}.$$

We see that a cannot be 0, and there $q-1$ choices for a. There are a total of q^2-q choices for b and d together. Then, we divide by $q-1$ for γ to be an element of $\mathrm{PGL}_2(k)$. Since there are $(q^2-q)/2$ pairs of elements of $\mathbb{F}_{q^2}\backslash\mathbb{F}_q$, then

$$|\Gamma_W| = \frac{(q^2-q)}{(q^2-q)/2} = 2.$$

For the $(\epsilon,\epsilon,\epsilon)$ cubic case, we choose $W = \{\theta, \theta', \theta''\}$. Consider $\gamma \in \Gamma_W$ which are of the form in Equation 1. We map triples of θ, θ', and θ'' to some other triple of elements of $\mathbb{F}_{q^3}\backslash\mathbb{F}_q$. There are $(q^3-q)/3$ triples in $\mathbb{F}_{q^3}\backslash\mathbb{F}_q$, so the total number of such γ is

$$|\Gamma_W| = \frac{|\mathrm{PGL}_2(k)|}{(q^3-q)/3} = 3.$$

□

3.2. Arbitrary Prime p, Four Branch Points

In general, the four-branch point case is more complicated. The non-split cases are more intricate than the split cases, so we consider them separately.

3.2.1. Split Cases.

Proposition 3.2.2. *Consider the ramification divisor* $(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4)$ *split.*

For $p = 2$*, the following gives the weighted sum of Artin-Schreier covers up to* k*-isomorphism:*

$$\sum_{[C]} \frac{1}{|\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle|} =$$

Ramification Divisor	*Weighted Number of Covers*	
	$q \equiv 1 \bmod 3$	$q \equiv -1 \bmod 3$
$(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4)$	$(q-1)^4 q^E (q+2)/6$	$(q-1)^4 q^E (q-2)/6$
$(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_3)$	$(q-1)^4 q^E (q+2)/6$	$(q-1)^4 q^E (q-2)/6$
$(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_2)$	$(q-1)^4 q^E (q-2)/6$	$(q-1)^4 q^E (q-2)/6$
$(\epsilon_1, \epsilon_1, \epsilon_2, \epsilon_2)$	$(q-1)^4 q^E (q+2)/12$	$(q-1)^4 q^E (q-2)/12$
$(\epsilon, \epsilon, \epsilon, \epsilon)$	$(q-1)^4 q^E (q-2)/24$	$(q-1)^4 q^E (q-2)/24$

For $p = 3$*, the following gives the weighted sum of Artin-Schreier covers up to* k*-isomorphism:*

$$\sum_{[C]} \frac{1}{|\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle|} =$$

Ramification Divisor	*Weighted Number of Covers*
$(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4)$	$(q-1)^4 q^E (q+3)/6$
$(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_3)$	$(q-1)^4 q^{E+1}/6$
$(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_2)$	$(q-1)^4 q^E (q-2)/6$
$(\epsilon_1, \epsilon_1, \epsilon_2, \epsilon_2)$	$(q-1)^4 q^{E+1}/12$
$(\epsilon, \epsilon, \epsilon, \epsilon)$	$(q-1)^4 q^E (q-2)/24$

For $p \geq 5$, the following gives the weighted sum of Artin-Schreier covers up to k-isomorphism:

$$\sum_{[C]} \frac{1}{|\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle|} =$$

Ramification Divisor	*Weighted Number of Covers*	
	$q \equiv 1 \bmod 3$	$q \equiv -1 \bmod 3$
$(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4)$	$(q-1)^4 q^E (q+5)/6$	$(q-1)^4 q^E (q+1)/6$
$(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_3)$	$(q-1)^4 q^E (q+2)/6$	$(q-1)^4 q^E (q-2)/6$
$(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_2)$	$(q-1)^4 q^E (q-4)/6$	$(q-1)^4 q^E (q-4)/6$
$(\epsilon_1, \epsilon_1, \epsilon_2, \epsilon_2)$	$(q-1)^4 q^E (q+2)/12$	$(q-1)^4 q^E (q-2)/12$
$(\epsilon, \epsilon, \epsilon, \epsilon)$	$(q-1)^4 q^E (q-6)/24$	$(q-1)^4 q^E (q-2)/24$

PROOF. We can choose $W = \{\infty, 0, 1, t\}$ because the action of $\mathrm{PGL}_2(k)$ is triply transitive [13], which implies that there is always an element t in an orbit with $\{\infty, 0, 1\}$. Using Theorem 2.5.2, the weighted sum equals

$$\frac{|\mathcal{N}_{W,t}|}{p} \sum_H \frac{|\theta_H|}{|H|}$$

where $|\mathcal{N}_{W,t}|$ is the number of rational functions $u(x)$ branched at W including the point t and having poles of order $\vec{\epsilon}$. By Lemma 2.3.1 and Corollary 2.3.3, $|\mathcal{N}_{W,t}| = p(q-1)^4 q^{E(\epsilon_1,\epsilon_2,\epsilon_3,\epsilon_4)}$.

H is a subgroup of S_4, and θ_H is the set of orbits of t for which $H = \Gamma_{W,t}$, the subset of $\mathrm{PGL}_2(k)$ which fixes W. Note that we only need to compute

$$\sum_H \frac{|\theta_H|}{|H|}.$$

We can find $|H|$ based on some conditions of what t must be. Finally, we combine the terms according to Theorem 2.5.2.

TABLE 3.3. $|H|$ for 4-Branch Point Split Cases in which $p = 2$

Case	Conditions	$\lvert H\rvert$
$(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4)$	none	1
$(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_3)$	none	1
$(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_2)$	$t = \zeta_3, \zeta_3^2$, $q \equiv 1 \mod 3$	3
	other t	1
$(\epsilon_1, \epsilon_1, \epsilon_2, \epsilon_2)$	none	2
$(\epsilon, \epsilon, \epsilon, \epsilon)$	$t = \zeta_3, \zeta_3^2$, $q \equiv 1 \mod 3$	12
	$t \neq \zeta_3, \zeta_3^2$, $q \equiv 1 \mod 3$	4
	$q \equiv -1 \mod 3$	4

TABLE 3.4. $|H|$ for 4-Branch Point Split Cases in which p is Odd

Case	Conditions	$\lvert H\rvert$
$(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4)$	none	1
$(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_3)$	$t = -1$	2
	$t \neq -1$	1
$(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_2)$	$t = -1, 1/2$	6
	$t = \zeta_3, \zeta_3^2$	3
	other t	1
$(\epsilon_1, \epsilon_1, \epsilon_2, \epsilon_2)$	$t = -1$	4
	$t \neq -1$	2
$(\epsilon, \epsilon, \epsilon, \epsilon)$	$p = 3$, $t = 2$	24
	$p = 3$, $t \neq 2$	4
	$p \geq 5$, $t = \zeta_6, \zeta_6^2, \zeta_6^4, \zeta_6^5$	12
	$p \geq 5$, $t = 1/2, 2, -1$	8
	$p \geq 5$, other t	4

Notice that some of these cases depend on the choice of t, and we can determine $|\Gamma_{W,t}|$ by explicit computation. We consider the mappings of $\{\infty, 0, 1\}$, which are the six fractional linear transformations:

$$x \mapsto \{x, 1-x, 1/x, x/(x-1), 1/(1-x), (x-1)/x\}$$

where choices of $t \in k\backslash\{0,1\}$ fix the set of branch points under the mapping. In any of these cases, if the orders of two branch points are different, then the two points cannot be mapped to one another.

In particular, the $(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4)$ case only has the identity, the $(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_3)$ has mappings which ∞ and 0 can switch, and the $(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_2)$ can have all six mappings with an appropriate choice of t. All of these cases have $H \subseteq S_3$.

The $(\epsilon_1, \epsilon_1, \epsilon_2, \epsilon_2)$ can have mappings in which ∞ and 0 switch or 1 and t switch, so H is $C_2 \times C_2$.

On the other hand, the $(\epsilon, \epsilon, \epsilon, \epsilon)$ case is the most complicated, and $H = (C_2 \times C_2) \rtimes \Gamma'$ for Γ' in Lemma 3.2.3.

TABLE 3.5. H for 4-Branch Point Split Cases

Mapping	Points		Conditions			
Function	From	To	$p=2$	$p=3$	$p=5$	$p\geq 7$
$\gamma: x\mapsto x$	0	0	None	None	None	None
	1	1				
	∞	∞				
	t	t				
$\gamma: x\mapsto 1-x$	0	1	does not occur	$t=-1$	$t=1/2$	$t=1/2$
order 2	1	0				
	∞	∞				
	t	t				
$\gamma: x\mapsto 1/x$	0	∞	does not occur	$t=-1$	$t=-1$	$t=-1$
order 2	1	1				
	∞	0				
	t	t				
$\gamma: x\mapsto x/(x-1)$	0	0	does not occur	$t=-1$	$t=2$	$t=2$
order 2	1	∞				
	∞	1				
	t	t				
$\gamma: x\mapsto 1/(1-x)$	0	1	$t=\zeta_3,\zeta_3^2$	$t=-1$	$t=\zeta_6^i$	$t=\zeta_6^i$
order 3	1	∞			$i=1,2,4,5$	$i=1,2,4,5$
	∞	0				
	t	t				
$\gamma: x\mapsto (x-1)/x$	0	∞	$t=\zeta_3,\zeta_3^2$	$t=-1$	$t=\zeta_6^i$	$t=\zeta_6^i$
order 3	1	0			$i=1,2,4,5$	$i=1,2,4,5$
	∞	1				
	t	t				

□

LEMMA 3.2.3. *In the $(\epsilon,\epsilon,\epsilon,\epsilon)$ case, $C_2\times C_2$ is always a subset of $\Gamma_{W,t}$ for any $t\in k\backslash\{0,1\}$.*

PROOF. Given a $t\in k\backslash\{0,1\}$, define the following:

$$\gamma_1=\begin{pmatrix}0 & t\\ 1 & 0\end{pmatrix} \text{ and } \gamma_2=\begin{pmatrix}1 & -t\\ 1 & -1\end{pmatrix}$$

as matrix representations elements of $\mathrm{PGL}_2(k)$.

Note that

$$\gamma_1 = \begin{pmatrix} 0 & t \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} t \\ x \end{pmatrix} \text{ or that } \gamma_1 : x \mapsto \frac{t}{x},$$

so $\gamma_1(\infty) = 0, \gamma_1(0) = \infty, \gamma_1(1) = t$, and $\gamma_1(t) = 1$. Similarly,

$$\gamma_2 = \begin{pmatrix} 1 & -t \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} x - t \\ x - 1 \end{pmatrix} \text{ or that } \gamma_1 : x \mapsto \frac{x-t}{x-1},$$

so $\gamma_1(\infty) = 1, \gamma_1(1) = \infty, \gamma_1(0) = t$, and $\gamma_1(t) = 0$.

We check the orders of γ_1 and γ_2:

$$\gamma_1 = \begin{pmatrix} 0 & t \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & t \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix}$$

and

$$\gamma_2 = \begin{pmatrix} 1 & -t \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & -t \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1-t & 0 \\ 0 & 1-t \end{pmatrix}.$$

Since $\gamma_1, \gamma_2 \in \mathrm{PGL}_2(k)$, then the order of each is 2.

In addition, note that

$$\gamma_1 \circ \gamma_2 = \begin{pmatrix} 0 & t \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -t \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} t & -t \\ 1 & -t \end{pmatrix} = \begin{pmatrix} 1 & -t \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & t \\ 1 & 0 \end{pmatrix} = \gamma_2 \circ \gamma_1 := \gamma_3.$$

So the group generated by γ_1 and γ_2 is $C_2 \times C_2$. Furthermore, γ_3 is the mapping in which

$$\gamma_3 : x \mapsto \frac{tx - t}{x - t},$$

meaning $\gamma_3(0) = 1, \gamma_3(1) = 0, \gamma_3(\infty) = t$, and $\gamma_3(t) = \infty$. □

PROOF. By explicit computation and because of Lemma 3.2.3, $H = (C_2 \times C_2) \rtimes \Gamma'$ where Γ' is:

TABLE 3.6. H for 4-Branch Point $(\epsilon, \epsilon, \epsilon, \epsilon)$ Split Cases

Prime	Condition	Γ'
$p = 2$	$t = \zeta_3, \zeta_3^2$	$\{x, 1/(1-x), (1-x)/x\}$
	other t	$\{x\}$
$p = 3$	$t = 2 = -1$	$\cong S_3$
	$t \neq 2$	$\{x\}$
$p \geq 5$	$t = \zeta_6, \zeta_6^2, \zeta_6^4, \zeta_6^5$	$\{x, 1/(1-x), (1-x)/x\}$
	$t = 1/2, 2$ or -1	C_2
	all other t	$\{x\}$

□

The number of orbits is dependent on t as well as p and q.

LEMMA 3.2.4. *[8, Theorem C] The numbers of orbits of 4-sets of* $\mathbb{P}^1(k)$ *under* $\mathrm{PGL}_2(k)$ *are:*

TABLE 3.7. Number of Orbits of $\mathbb{P}^1(k)$ Under $\mathrm{PGL}_2(k)$

Prime	*Condition*	*Orbits*
$p = 2$	$q \equiv 1 \bmod 3$	$(q+2)/6$
	$q \equiv -1 \bmod 3$	$(q-2)/6$
$p = 3$	*any* q	$(q+3)/6$
$p \geq 5$	$q \equiv 1 \bmod 3$	$(q+5)/6$
	$q \equiv -1 \bmod 3$	$(q+1)/6$

Also, we have the following cases that appear in our choices for t: t is a 3rd root of unity, t is a 6th root of unity, or $t = 1/2, 2$, or -1. For such cases, we use the following:

LEMMA 3.2.5. *Given* $t \in k \backslash \{0, 1\}$.

(1) If $p = 2$, *then* $t = \zeta_3$ *and* $t = \zeta_3^2$ *are in the same orbit under* $\mathrm{PGL}_2(k)$.

(2) If $p \geq 5$, *then we have two orbits of sixth roots not equal to* ± 1 *under* $\mathrm{PGL}_2(k)$: $t = \zeta_6$ *and* $t = \zeta_6^5$ *as well as* $t = \zeta_6^2$ *and* $t = \zeta_6^4$.

(3) If $p \geq 5$, $t = 1/2, 2$, *and* -1 *are in the same orbit under* $\mathrm{PGL}_2(k)$.

PROOF. The cross-ratio is preserved by fractional linear transformations, which are the elements of $\mathrm{PGL}_2(k)$. Thus, we just have to show that one value of t is mapped to another under some $\gamma \in \mathrm{PGL}_2(k)$.

(1) Note that $\gamma(x) = 1/x$ takes $t = \zeta_3$ to $t = \zeta_3^2$.

(2) Similarly, $\gamma(x) = 1/x$ takes $t = \zeta_6$ to $t = \zeta_6^5$ and $t = \zeta_6^2$ to $t = \zeta_6^4$.

(3) For $t = 1/2, 2$, or -1, we have the following:

$$\begin{aligned} \gamma(x) &= 1/x \text{ takes } 2 \mapsto 1/2 \\ \gamma(x) &= 1 - x \text{ takes } 2 \mapsto -1 \end{aligned}$$

□

Two explicit applications of Theorem 2.5.2 are below.

PROOF. $(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_3)$ with $p = 3$:

Recall that $|\mathcal{N}_{W,t}| = p(q-1)^4 q^{E(\epsilon_1,\epsilon_2,\epsilon_3,\epsilon_3)}$. The sizes of the orbits are different depending on our choice of t. In particular, if $t = -1$, then $|H| = 2$ whereas if $t \neq -1$, then $|H| = 1$. There is one orbit with $t = -1$ and $(q+3)/6 - 1$ orbits in which $t \neq -1$. The total weighted sum of covers is:

$$\frac{p(q-1)^4 q^{E(\epsilon_1,\epsilon_2,\epsilon_3,\epsilon_3)}}{p}\left(\frac{1}{2} + \frac{q+3}{6} - 1\right) = \frac{(q-1)^4 q^{E(\epsilon_1,\epsilon_2,\epsilon_3,\epsilon_3)+1}}{6}.$$

□

PROOF. $(\epsilon, \epsilon, \epsilon, \epsilon)$ with odd $p \geq 5$ and $q \equiv 1 \mod 3$:

As with the previous example, $|\mathcal{N}_{W,t}| = p(q-1)^4 q^{E(\epsilon,\epsilon,\epsilon,\epsilon)}$. If t is a 6th root, then $|H| = 12$. If $t = 1/2, 2, -1$, then $|H| = 8$. Otherwise, the $|H| = 4$. There are two orbits with the 6th roots, one with $t = 1/2, 2, -1$ and $(q+5)/6 - 3$ orbits otherwise. The total weighted sum of covers is:

$$\frac{p(q-1)^4 q^{E(\epsilon,\epsilon,\epsilon,\epsilon)}}{p}\left(\frac{2}{12} + \frac{1}{8} + \frac{1}{4}\left(\frac{q+5}{6} - 3\right)\right) = \frac{(q-1)^4 q^{E(\epsilon,\epsilon,\epsilon,\epsilon)}(q-6)}{24}.$$

□

3.2.6. Number of Orbits for Non-Split Cases. We begin by describing the number of orbits for 4-sets under $\mathrm{PGL}_2(k)$.

Lemma 3.2.7. *[10, Proposition 2.3] The numbers of orbits of our 4-sets under* $\mathrm{PGL}_2(k)$ *are:*

Table 3.8. Subcases for the Number of Orbits of $\mathbb{P}^1(\overline{k})$ Under $\mathrm{PGL}_2(k)$ for $p = 2$

Case	*Orbits*
Split	$(q-2)/6 + \left[\frac{2}{3}\right]_{meven}$
Split + Quadratic	$q/2$
Quadratic	$q/2 - 1$
Cubic	$(q+1)/3 + \left[\frac{4}{3}\right]_{meven}$
Quartic	$q/2$

Note that the total number of orbits is $2q+1$ if $q \equiv 1 \bmod 3$ and $2q-1$ if $q \equiv -1 \bmod 3$.

Theorem 3.2.8. *[7, Theorem 2.2] The numbers of orbits of* 4*-sets of* $\mathbb{P}^1(\overline{k})$ *under* $\mathrm{PGL}_2(k)$ *are:*

Table 3.9. Number of Orbits of $\mathbb{P}^1(\overline{k})$ Under $\mathrm{PGL}_2(k)$

Prime	*Condition*	*Orbits*
$p = 3$	$q \equiv 1 \bmod 4$	$2q+2$
	$q \equiv -1 \bmod 4$	$2q+1$
$p \geq 5$	$q \equiv 1 \bmod 3$	$2q+3$
	$q \equiv -1 \bmod 3$	$2q+1$

We summarize the number of orbits for each case:

Theorem 3.2.9. *The number of orbits of* 4*-sets of* $\mathbb{P}^1(\overline{k})$ *under* $\mathrm{PGL}_2(k)$ *are:*

TABLE 3.10. Subcases for the Number of Orbits of $\mathbb{P}^1(\overline{k})$ Under $\mathrm{PGL}_2(k)$ for Odd p

Prime	*Condition*	*Split*	*Split+Quad*	*Quadratic*	*Cubic*	*Quartic*
3	$q \equiv 1 \bmod 4$	$(q+3)/6$	$(q+1)/2$	$(q-1)/2$	$(q+3)/3$	$(q+1)/2$
	$q \equiv -1 \bmod 4$	$(q+3)/6$	$(q+1)/2$	$(q-1)/2$	$(q+3)/3$	$(q-1)/2$
≥ 5	$q \equiv 1 \bmod 3$	$(q+5)/6$	$(q+1)/2$	$(q-1)/2$	$(q+5)/3$	$(q+1)/2$
	$q \equiv -1 \bmod 3$	$(q+1)/6$	$(q+1)/2$	$(q-1)/2$	$(q+1)/3$	$(q+1)/2$

We use Burnside's Lemma to determine the number of orbits. Let Γ be a group acting on a set I. Let $|I/\Gamma|$ denote the number of orbits of I under Γ, and $|\mathrm{Fix}_\gamma|$ denote the number of elements of I fixed by $\gamma \in \Gamma$. Then

$$|I/\Gamma| = \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} |\mathrm{Fix}_\gamma|.$$

3.2.9.1. *Split+Quadratic Case:* We choose $W = \{\infty, 0, \theta, \theta'\}$ where $\theta, \theta' \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ are the roots of an irreducible monic quadratic polynomial $f(x) \in k[x]$.

Case: $(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_3)$ or $(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_2)$

We must have $0 \mapsto 0, \infty \mapsto \infty$, meaning our possible $\gamma \in \Gamma_W$ is $\gamma : x \mapsto ax$. So, $|\Gamma_W| = q - 1$ here.

- Case 1: $I = \{f(x) = x^2 - A \mid A \in k \text{ is not a square}\}$. The number of such $f(x)$ is $(q-1)/2$.

$$\frac{f(ax)}{a^2} = \frac{a^2x^2 - A}{a^2} = x^2 - \frac{A}{a^2} \overset{set}{=} x^2 - A$$

Thus, $a = \pm 1$ and each one of these γ fixes all $(q-1)/2$ elements, so

$$|I/\Gamma_W| = \frac{1}{q-1}\left(\frac{q-1}{2} + \frac{q-1}{2}\right) = 1.$$

- Case 2: $I = \{f(x) = x^2 + Ax + B \mid A, B \in k, A \neq 0 \text{ and } f(x) \text{ is irreducible}\}$. The number of such $f(x)$ is

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

which we determine by subtracting Case 1 from the total number of irreducible degree two polynomials.

$$\frac{f(ax)}{a^2} = x^2 + \frac{Ax}{a} + \frac{B}{a^2} \overset{set}{=} x^2 + Ax + B$$

so $a = 1$ must be true, and the identity element fixes everything. This implies that the total number of orbits is

$$|I/\Gamma_W| = \frac{1}{q-1}\left(\frac{(q-1)^2}{2}\right) = \frac{q-1}{2}.$$

Hence, the number of orbits for the case is

$$1 + \frac{q-1}{2} = \frac{q+1}{2}.$$

Case: $(\epsilon_1, \epsilon_1, \epsilon_2, \epsilon_2)$ or $(\epsilon, \epsilon, \epsilon, \epsilon)$

Note that we could either have $0 \mapsto 0, \infty \mapsto \infty$ or $0 \mapsto \infty, \infty \mapsto 0$ if the orders of the two are the same, meaning our possible $\gamma \in \Gamma$ are $\gamma_1 : x \mapsto ax$ or $\gamma_2 : x \mapsto b/x$ for $a, b \in k$. So, $|\Gamma_W| = 2(q-1)$ here.

- Case 1: $I = \{f(x) = A_0x^2 - A \mid A_0, A \in k^*, f(x) \text{ is irreducible}\}$. Note that if we look for the roots, we get the equations $A_0x^2 - A = 0 \Rightarrow x^2 = A/A_0$. Thus, two elements $f(x) = A_0x^2 - A$ and $g(x) = B_0x^2 - B$ are equivalent if $A/A_0 = B/B_0$. The number of such $f(x)$ is $(q-1)/2$.

$$\frac{f(ax)}{a^2} = A_0x^2 - \frac{A}{a^2} \stackrel{set}{=} 0$$

which implies $x^2 = A/(A_0a^2)$. To have any elements fixed, we must have $A/(A_0a^2) = A/A_0$ or $a = \pm 1$. Each one of these elements fixes all $(q-1)/2$ elements.

We also have

$$x^2 f\left(\frac{b}{x}\right) A_0b^2 - Ax^2 \stackrel{set}{=} 0$$

which implies $x^2 = A_0b^2/A$. If any element of I is fixed, then we have $A_0b^2/A = A/A_0$ or that $b = \pm A/A_0$.

If -1 is a square in k, then A/A_0 is a square if and only if $-A/A_0$ is also a square. There are $(q-1)/2$ such choices of squares for b, and there are two elements fixed for each of these choices of b. If -1 is not a square in k, then A/A_0 is a square exactly when $-A/A_0$ is not, so we have $q-1$ choices of b that fix one element each.

The total number of orbits is

$$|I/\Gamma_W| = \frac{1}{2(q-1)}\left(\frac{q-1}{2}(2) + (q-1)(1)\right) = 1.$$

- Case 2: $I = \{f(x) = x^2 + Ax + B \mid A, B \in k \text{ and } f(x) \text{ is irreducible}\}$. The number of such $f(x)$ is

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

$$\frac{f(ax)}{a^2} = x^2 + \frac{Ax}{a} + \frac{B}{a^2} \overset{set}{=} x^2 + Ax + B$$

so $a = 1$ must be true, and this fixes all elements.

We also have:

$$x^2 f\left(\frac{b}{x}\right) = Bx^2 + Abx + b^2 \overset{set}{0} x^2 + Ax + B$$

so $B = 1$ and $b = 1$ must be true, and this also fixes all elements. Thus,

$$|I/\Gamma_W| = \frac{1}{2(q-1)}\left(\frac{(q-1)^2}{2} + \frac{(q-1)^2}{2}\right) = \frac{q-1}{2}.$$

Hence, the number of orbits is $1 + (q-1)/2 = (q+1)/2$.

3.2.9.2. *Quadratic Case:* This includes both the $(\epsilon_1, \epsilon_1, \epsilon_2, \epsilon_2)$ case and the $(\epsilon, \epsilon, \epsilon, \epsilon)$ case. We choose $W = \{\theta, \theta', \tau, \tau'\}$ where $\theta, \theta', \tau, \tau' \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. Note that $\{\theta, \theta'\}$ and $\{\tau, \tau'\}$ are the pairs of roots for irreducible monic quadratic polynomials, which we call $f_1(x)$ and $f_2(x)$. Consider $f(x) = f_1(x)f_2(x)$ over $\mathbb{F}_q = k$. Every orbit under $\mathrm{PGL}_2(k)$ contains one such $f(x)$ with $f_1(x) = x^2 - s$ with roots $\pm\sqrt{s}$ where s is not a square in k.

We first consider γ which fix f_1. We compute

$$\begin{aligned}(cx+d)^2 f_1\left(\frac{ax+b}{cx+d}\right) &= (a^2x^2+2abx+b^2)-x(c^2x^2+2cdx+d^2)\\ &= x^2(a^2-sc^2)+x(2ab-2cds)+b^2-sd^2\\ &\stackrel{set}{=} x^2-s\end{aligned}$$

which we simplify by using the relation $x^2-s=0$ or $x^2=s$. This implies that $2ab-2cds=0$ or $ab=cds$ and $b^2-sd^2+sa^2-s^2c^2=0$.

If $a=0$, then $cds=0$. Since $c\neq 0$ and $s\neq 0$, then $d=0$ must be true. So we have $b^2-s^2c^2=0$ or $b=\pm sc$.

Note that if $a\neq 0$, then $b=cds/a$ and

$$\begin{aligned}c^2d^2s^2-sa^2d^2+sa^4-s^2c^2a^2 &= 0\\ s(a^2-sc^2)(a^2-d^2) &= 0\end{aligned}$$

Since $s\neq 0$ and $a^2-sc^2\neq 0$ since s is not a square in k, then $a^2-d^2=0$ or $a=\pm d$. Thus, the only possibilities for mappings to fix f_1 are:

$$\gamma_1=\begin{pmatrix} a & cs\\ c & a\end{pmatrix} \text{ and } \gamma_2=\begin{pmatrix} a & -cs\\ c & -a\end{pmatrix}$$

for $a,c\in k$ not both equal to 0.

Note that γ_1 fixes $\sqrt{s}$ and $-\sqrt{s}$, and γ_2 swaps the two roots. Also, the size of the equivalence classes in $\mathrm{PGL}_2(k)$ for each γ_i is $(q^2-1)/(q-1)=q+1$.

Now we apply γ_1 and γ_2 to $f_2=x^2+Ax+B$ for $A,B\in k$.

For γ_1, we compute:

$$\begin{aligned}(cx+a)^2 f_2\left(\frac{ax+cs}{cx+a}\right) &= x^2(a^2+Aac+Bc^2)+x(2acs+Aa^2+Ac^2s+2Bac)\\ &\quad +c^2s^2+Aacs+Ba^2\\ &\stackrel{set}{=} \lambda(x^2+Ax+B)\end{aligned}$$

for some scaling factor $\lambda \in k^*$.

Equating the coefficients for the leading terms, we get $a^2+Aac+Bc^2=\lambda$. This gives the following two equations from the linear and constant terms:

$$\begin{aligned}A^2ac+ABc^2-2acs-Ac^2s-2Bac &= 0\\ ABac+B^2c^2-c^2s^2-Aacs &= 0\end{aligned}$$

- Case 1: $c=0$ yields the identity map, so γ_1 fixes all possible $(q+1)(q-2)/2$ quadratic polynomials for f_2.
- Case 2: If $c \neq 0$, then we can divide by c and get the conditions

$$\begin{aligned}Ac(B-s)-2a(B+s)+A^2a &= 0\\ c(B^2-s^2)+Aa(B-s) &= 0\end{aligned}$$

  - Suppose $a=0$. Without loss of generality, let $c=1$. We get the conditions:

$$\begin{aligned}A(B-s) &= 0\\ B^2-s^2 &= 0\end{aligned}$$

which imply that $B = \pm s$. If $B = -s$, then $A = 0$, but then $f_2 = x^2 - s = f_1$, so this is impossible. Thus, $B = s$ must be true and $f_2 = x^2 + Ax + s$. We count the number of such quadratic polynomials which are irreducible, which is dependent on when $A^2 - 4s$ is not a square. Alternatively, we can count the number N of $(A/2)^2 - s$ which are not a square. First, we consider $N = q - M$ where

$$\begin{aligned} M &= \#\{A \in k \mid A^2 - 4s = t^2 \in k\} \\ &= \#\{\underline{A} \in k \mid \underline{A}^2 - s = t^2 \in k\} \end{aligned}$$

where $\underline{A} = A/2$.

Note that if $t = 0$, then $\underline{A}^2 = s$, but this is impossible since s cannot be a square. We can therefore count the set

$$M' = \#\{(\underline{A}, t) \mid \underline{A}^2 - t^2 = s\},$$

and notice that if $(\underline{A}, t) \in M'$, then so is $(\underline{A}, -t)$, so $M' = 2M$.

Let $\underline{A}^2 = z$ and $t^2 = w$ where $z, w \in k$. We can rewrite M' as

$$\begin{aligned}
M' &= \sum_{z-w=s} \left(1 + \binom{z}{q}\right)\left(1 + \binom{w}{q}\right) \\
&= \sum_{z-w=s} \left(1 + \binom{z}{q} + \binom{w}{q} + \binom{z}{q}\binom{w}{q}\right) \\
&= \sum_{z-w=s} 1 + \sum_{z-w=s} \binom{z}{q} + \sum_{z-w=s} \binom{w}{q} + \sum_{z-w=s} \binom{z}{q}\binom{w}{q} \\
&= q + 0 + 0 + \sum_{z-w=s} \binom{zw}{q} \\
&= q + \sum_{z-w=s, w\neq 0} \binom{z/w}{q} \\
&= q + \sum_{z\neq s} \binom{z/(z-s)}{q}
\end{aligned}$$

Now let $y = z/(z-s)$. Solving for z, we get $z = sy/(y-1)$. So we have:

$$\begin{aligned}
M' &= q + \sum_{y\neq 1} \binom{y}{q} \\
&= q - \binom{1}{q} \\
&= q - 1
\end{aligned}$$

Thus, $M = (q-1)/2$, and $N = q - (q-1)/2 = (q+1)/2$.

– Suppose $a \neq 0$. There are $q-1$ choices for such automorphisms. Without loss of generality, let $a = 1$. Suppose $B \neq s$. Then our second equation becomes

$$c(B+s) + A = 0 \Rightarrow A = -c(B+s)$$

which we can substitute into the first equation to get

$$\begin{aligned} -c(B+s)/c(B-s) - 2(B+s) + (-c(B+s))^2 &= 0 \\ 2(B+s)(c^2 s - 1) &= 0 \end{aligned}$$

If $c^2 s - 1 = 0$, then $s = (1/c)^2$, but s cannot be a square, so this is not possible. Thus, $B + s = 0$ must be true, or $B = -s$, but then $f_2 = x^2 - s = f_1$. Therefore, this case does not occur.

Suppose $B = s$. Then we get the condition:

$$\begin{aligned} A^2 c - 4Bc &= 0 \\ &= c(A^2 - 4B) \end{aligned}$$

meaning that $A = \pm 2\sqrt{B}$. Thus, $f_2 = x^2 + 2\sqrt{B} + B = (x + \sqrt{B})^2$ or $f_2 = x^2 - 2\sqrt{B} + B = (x - \sqrt{B})^2$. Either way, f_2 is not irreducible, so this case does not occur.

To apply Burnside's Lemma, notice that since every orbit contains an element of the form $(x^2 - s)f_2$, then

$$I = \{f_2(x) = x^2 + Ax + B \mid f_2(x) \text{ irreducible}, f_2 \neq x^2 - s\}.$$

There are $(q^2 - q)/2 - 1 = (q+1)(q-2)/2$ choices for f_2, and there are $q + 1$ choices for γ_1. So we have

$$|I/\langle \gamma_1 \rangle| = \frac{1}{q+1}\left(\frac{(q+1)(q-2)}{2} + \frac{q+1}{2}\right) = \frac{q-1}{2}.$$

Now we consider the action of $x \mapsto -x$ on the orbits. Note that this is the γ_2 case when $c = 0$. We want to check if $f_2(\gamma_1(x)) = -1 \cdot f_2(x)$ for some (a, c), or that $x^2 + Ax + B$ and $x^2 - Ax + B$ are in the same orbit under $\langle \gamma_1 \rangle$. If so, then γ_2 does not change the number of orbits for the quadratic case that was computed above for γ_1, implying that the number of orbits under $\{\gamma_1, \gamma_2\}$ would be the same as the number of orbits under $\{\gamma_1\}$.

$$\begin{aligned} f_2\left(\frac{ax+cs}{cx+a}\right) &= x^2(a^2 + Aac + Bc^2) + x(2acs + Aa^2 + Ac^2s + 2Bac) \\ &\quad +(c^2s^2 + Aacs + Ba^2) \\ &\Rightarrow x^2 + x\left(\frac{2acs + Aa^2 + Ac^2s + 2Bac}{a^2 + Aac + Bc^2}\right) + \frac{c^2s^2 + Aacs + Ba^2}{a^2 + Aac + Bc^2} \\ &\overset{set}{=} x^2 - Ax + B \end{aligned}$$

so then

$$\begin{aligned} B &= \frac{c^2s^2 + Aacs + Ba^2}{a^2 + Aac + Bc^2} \\ Ba^2 + ABac + B^2c^2 &= c^2s^2 + Aacs + Ba^2 \\ 0 &= B^2c^2 + BAac - Aacs - c^2s^2 \end{aligned}$$

which is the same condition as mentioned earlier for the constant term.

For the linear term, we have:

$$\begin{aligned} -A &= \frac{2acs + Aa^2 + Ac^2s + 2Bac}{a^2 + Aac + Bc^2} \\ -Aa^2 - A^2ac - ABc^2 &= 2acs + Aa^2 + Ac^2s + 2Bac \\ 0 &= a^2(2A) + a(2cs + 2Bc + A^2c) + Ac^2s + ABc^2 \end{aligned}$$

We can solve for a using the quadratic formula, and we want

$$(2cs + 2Bc + A^2c)^2 - 4(2A)(Ac^2s + ABc^2) = c^2((A^2 + 2(B + s))^2 - 8A^2(B + s))$$

to be a square. In other words, we want

$$(A^2 + 2(B + s))^2 - 8A^2(B + s) = (A^2 - 2(B + s))^2$$

to be a square, which is clear. Hence, given A and B, we can find an a which works, and $x^2 + Ax + B$ and $x^2 - Ax + B$ are in the same orbit under $\langle\gamma_1\rangle$. Therefore, the total number of orbits of the quadratic case under $\mathrm{PGL}_2(k)$ is exactly $(q-1)/2$.

3.2.9.3. *Cubic Case:* This includes both the $(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_2)$ case and the $(\epsilon, \epsilon, \epsilon, \epsilon)$ case. We choose $W = \{\infty, \theta, \theta', \theta''\}$ where $\theta, \theta', \theta'' \in \mathbb{F}_{q^3} \backslash \mathbb{F}_q$ and are the roots of an irreducible monic cubic polynomial $f(x) \in k[x]$.

Note that if $\gamma \in \Gamma_W$, then ∞ must be fixed, so possible $\gamma \in \Gamma_W$ are of the form $\gamma : x \to ax + b$ for $a \in k^*, b \in k$, and $|\Gamma_W| = q(q-1)$.

Let $f(x) = x^3 + Ax^2 + Bx + C \in k[x]$. Then

$$I = \{f(x) = x^3 + Ax^2 + Bx + C \mid A, B, C \in k, f(x) \text{ irreducible}\}.$$

Case: $p \neq 3$

$$\begin{aligned}
\frac{f(ax+b)}{a^3} &= \frac{a^3x^3 + 3a^2bx^2 + 3ab^2x + b^3 + Aa^2x^2 + 2Aabx + Ab^2 + Bax + Bb + C}{a^3} \\
&= x^3 + x^2\left(\frac{3b+A}{a}\right) + x\left(\frac{3b^2+2Ab+B}{a^2}\right) + \frac{b^3+Ab^2+Bb+C}{a^3} \\
&\stackrel{set}{=} x^3 + Ax^2 + Bx + C
\end{aligned}$$

Equating coefficients, if $f(x) \in \text{Fix}_\gamma$, then:

$$\begin{aligned}
A &= \frac{3b+A}{a} \\
B &= \frac{3b^2+2Ab+B}{a^2} \\
C &= \frac{b^3+Ab^2+Bb+C}{a^3}
\end{aligned}$$

Now consider the subcases:

- Case 1: $a = 1, b = 0$. This means $\gamma : x \mapsto x$ and we have the identity map, so $|\text{Fix}_\gamma| = (q^3 - q)/3$ or the number of cubic monic irreducible polynomials.
- Case 2: $a = 1, b \neq 0$. This means $\gamma : x \mapsto x + b$. Immediately, we have the equation $3b + A = A \Rightarrow b = 0$, which is a contradiction. This case does not occur.
- Case 3: $a^3 \neq 1, a \neq -1$. Solving for A, B, and C, we get:

$$\begin{aligned}
A &= \frac{3b+A}{a} \\
Aa &= 3b + A \\
A(a-1) &= 3b \\
A &= \frac{3b}{a-1}
\end{aligned}$$

$$
\begin{aligned}
B &= \frac{3b^2 + 2\left(3b/(a-1)\right)b + B}{a^2} \\
Ba^2 - B &= 3b^2 + \frac{6b^2}{a-1} \\
B(a^2-1) &= 3b^2 + \frac{6b^2}{a-1} \\
B &= \frac{3b^2}{a^2-1} + \frac{6b^2}{(a-1)(a^2-1)} \\
&= \frac{3ab^2 - 3b^2 + 6b^2}{(a-1)^2(a+1)} \\
&= \frac{3b^2(a+1)}{(a-1)^2(a+1)} \\
&= \frac{3b^2}{(a-1)^2}
\end{aligned}
$$

$$
\begin{aligned}
C &= \frac{b^3 + 3b^3/(a-1) + 3b^2/(a-1)^2 + C}{a^3} \\
Ca^3 - C &= b^3 + \frac{3b^3}{a-1} + \frac{3b^3}{(a-1)^2} \\
C(a^3-1) &= b^3 + \frac{3b^3}{a-1} + \frac{3b^3}{(a-1)^2} \\
C &= \frac{b^3}{a^3-1} + \frac{3b^3}{(a-1)(a^3-1)} + \frac{3b^3}{(a-1)^2(a^3-1)} \\
&= \frac{b^3(a^2-2a+1) + 3ab^3 - 3b^3 + 3b^3}{(a-1)^2(a^3-1)} \\
&= \frac{a^2b^3 - 2ab^3 + b^3 + 3ab^3}{(a-1)^2(a^2+a+1)} \\
&= \frac{b^3(a^2+a+1)}{(a-1)^2(a^2+a+1)} \\
&= \frac{b^3}{(a-1)^3}
\end{aligned}
$$

These computations show that $a \neq -1$ and $a^3 \neq 1$ must be true if $a \neq 1$. Now we depress the cubic with the substitution $x = y - A/3$ to get

$$\begin{aligned} f(y) &= y^3 + C + \frac{2A^3}{27} - \frac{AB}{3} \\ &= y^3 + C + \frac{2(27)b^3}{27(a-1)^3} - \frac{3b}{3(a-1)}\left(\frac{3b^2}{(a-1)^2}\right) \\ &= y^3 + C + \frac{2b^3 - 3b^3}{(a-1)^3} \\ &= y^3 + \frac{b^3}{(a-1)^3} - \frac{b^3}{(a-1)^3} \\ &= y^3 \end{aligned}$$

which is clearly not irreducible, so this case does not occur for these values of a.

- Case 4: If $a = -1$, then we have $\gamma(x) = -x + b$. Notice that $\gamma^2 = x$, so the mapping is of order 2, but this is impossible for the cubic case since W contains $\theta, \theta', \theta''$ and γ cannot fix only one of these points.

If $a^3 = 1$, then we have

$$\begin{aligned} A &= \frac{3b}{a-1} \\ B &= \frac{3b^2}{(a-1)^2} \end{aligned}$$

and there is no condition on C, so we have

$$f(x) = x^3 + \frac{3b}{a-1}x^2 + \frac{3b^2}{(a-1)^2}x + C.$$

Depressing the cubic, we get

$$f(y) = y^3 + C - \left(\frac{b}{a-1}\right)^3,$$

so we only need to count the number of possibilities for the constant term to be a non-cube. If $q \equiv 1 \mod 3$, there are $2(q-1)/3$ choices. If $q \equiv -1 \mod 3$, there are no possibilities for non-cubes. Since there are two choices for a in which $a \neq 1$ and q choices for b, then we have a total of $4q(q-1)/3$ fixed elements when $q \equiv 1 \mod 3$.

Hence, the total number of orbits is

$$|I/\Gamma_W| = \begin{cases} \dfrac{1}{q(q-1)}\left(\dfrac{q^3-q}{3} + \dfrac{4q(q-1)}{3}\right) = \dfrac{q+5}{3} & q \equiv 1 \bmod 3 \\ \dfrac{1}{q(q-1)}\left(\dfrac{q^3-q}{3}\right) = \dfrac{q+1}{3} & q \equiv -1 \bmod 3 \end{cases}$$

Case: $p = 3$

$$\begin{aligned} \frac{f(ax+b)}{a^3} &= \frac{a^3x^3 + 3a^2bx^2 + 3ab^2x + b^3 + Aa^2x^2 + 2Aabx + Ab^2 + Bax + Bb + C}{a^3} \\ &= x^3 + x^2\left(\frac{A}{a}\right) + x\left(\frac{2Ab+B}{a^2}\right) + \frac{b^3 + Ab^2 + Bb + C}{a^3} \overset{set}{=} x^3 + Ax^2 + Bx + C \end{aligned}$$

Equating coefficients, if $f(x) \in \mathrm{Fix}_\gamma$, then:

$$\begin{aligned} A &= \frac{A}{a} \\ B &= \frac{2Ab+B}{a^2} \\ C &= \frac{b^3 + Ab^2 + Bb + C}{a^3} \end{aligned}$$

- Case 1: $a = 1, b = 0$. We have $I = \{f(x) = x^3 + Ax^2 + Bx + C \mid f(x) \text{ is irreducible}\}$, so $|I| = (q^3 - q)/3$, and the identity fixes all of these elements.

- Case 2: $a = 1, b \neq 0$. We have $2Ab + B = B \Rightarrow 2Ab = 0 \Rightarrow A = 0$. Also, $b^3 + Bb + C = C \Rightarrow b(b^2 + B) = 0 \Rightarrow b^2 + B = 0 \Rightarrow B = -b^2$.

  Thus, we are considering $I = \{f(x) = x^3 - b^2x + C \mid f(x) \text{ is irreducible}\}$. Note that there are $q - 1$ choices of C. By Theorem 2 in [14], this is equivalent to considering $\{f(x) = x^3 - b^2x + C \mid \text{tr}(C/b^3) \neq 0\}$. Consider $S = \{C \mid \text{tr}(C/b^3) = 0\}$. We show that S is a subgroup of index 3 in k.

  First, let $C_1, C_2 \in S$. Then since

$$\begin{aligned} \text{tr}(C_1/b^3) + \text{tr}(C_2/b^3) &= \text{tr}((C_1 + C_2)/b^3) \\ \text{tr}(C_1/b^3) + \text{tr}(-C_1/b^3) &= \text{tr}(0) = 0, \end{aligned}$$

  S is a subgroup of k.

  Now consider $C \in k$. We can write $C = \kappa^3$ in which $\kappa = \text{Frob}^{-1}(C)$ or $\text{Frob}(\kappa) = C$. Then

$$\begin{aligned} \text{tr}(C/b^3) &= \text{tr}(\kappa^3/b^3) \\ &= \text{tr}(\text{Frob}(\kappa/b)) \\ &= \text{tr}(\kappa/b) \end{aligned}$$

  since the trace is Frob-invariant. Thus, we can pick κ such that $\text{tr}(\kappa/b) \neq 0$, and the trace mapping is surjective. Because S is a subgroup of index 3 in k, then $|S| = q/3$ and the remaining $2q/3$ elements have nonzero trace. This means $|\{f(x) = x^3 - b^2x + C \mid \text{tr}(C/b^3) \neq 0\}| = 2q/3$.

We can now count the total number of orbits for the cubic case in which $p = 3$:

$$|I/\Gamma| = \frac{1}{q(q-1)}\left(\frac{q+1}{3} + (q-1)\left(\frac{2q}{3}\right)\right) = \frac{q+3}{3}.$$

3.2.9.4. *Quartic Case:* This occurs only for the $(\epsilon, \epsilon, \epsilon, \epsilon)$ case. We choose $W = \{\theta, \theta', \theta'', \theta'''\}$ where $\theta, \theta', \theta'', \theta''' \in \mathbb{F}_{q^4} \backslash \mathbb{F}_{q^2}$ are roots of the irreducible quartic polynomial $f(x) \in k[x]$. From [7, Theorem 2.2] and the above results, the number of orbits is completely determined here.

3.2.10. Weighted Sums for Nonsplit Cases.

Proposition 3.2.11. *For $p = 2$, the following gives the weighted number of Artin-Schreier covers up to k-isomorphism:*

$$\sum_{[C]} \frac{1}{|\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle|} =$$

Ramification Divisor	*Weighted Number of Covers*
$(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_3)$ *split+quad*	$(q-1)^2(q^2-1)q^{E+1}/4$
$(\epsilon_1, \epsilon_1, \epsilon_2, \epsilon_2)$ *quadratic*	$(q^2-1)^2 q^E (q-2)/4$
$(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_2)$ *cubic*	$(q-1)(q^3-1)q^E(q+1)/3$
$(\epsilon, \epsilon, \epsilon, \epsilon)$ *quartic*	$(q^4-1)q^{E+1}/4$

For odd p, the following gives the weighted number of Artin-Schreier covers up to k-isomorphism:

$$\sum_{[C]} \frac{1}{|\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle|} =$$

Ramification Divisor	*Weighted Number of Covers*
$(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_3)$ *split+quad*	$(q-1)^2(q^2-1)q^{E+1}/2$ *if* $\epsilon_1 \neq \epsilon_2$
	$(q-1)^2(q^2-1)q^{E+1}/4$ *if* $\epsilon_1 = \epsilon_2$
$(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_2)$ *cubic*	$(q-1)(q^3-1)(q+1)q^E/3$ *if* $p \neq 3, q \equiv 1 \mod 3$
	$(q-1)(q^3-1)(q+1)q^E/3$ *if* $p \neq 3, q \equiv -1 \mod 3$
	$(q-1)(q^3-1)(q+3)q^E/3$ *if* $p = 3$

PROOF. We fix the number n of branch points, the orders of the branch points, and the splitting behavior S to determine an appropriate rational equation. We choose the branch points, and we determine $|\mathcal{N}_W|$ with Lemma 2.3.1. Next, we find the number of orbits for which $\Gamma_W = H$ for each $H \subseteq S_n$ by explicitly computing $\gamma \in \Gamma$ of the form from Equation 1, given the restrictions imposed upon γ by the chosen branch points. Finally, we combine the terms according to Theorem 2.5.2.

TABLE 3.11. H and Number of Orbits for $p = 2$ Non-Split Cases

Case	H	Number of Orbits
$(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_3)$ split+quadratic	C_2	$q/2$
$(\epsilon_1, \epsilon_1, \epsilon_2, \epsilon_2)$ quadratic	$C_2 \times C_2$	$q/2 - 1$
$(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_2)$ cubic	μ_3 if $t = \infty$ when $q \equiv 1 \mod 3$	1
	μ_3 if $t = 0$ when $q \equiv 1 \mod 3$	1
	$\{1\}$	$(q+1)/3$
$(\epsilon, \epsilon, \epsilon, \epsilon)$ quartic	C_2	$q/2$

This table follows from [10, Section 3.1].

TABLE 3.12. H and Number of Orbits for Odd p Non-Split Cases

Case	H	Number of Orbits
$(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_3)$ split+quadratic	$\{x, -x\}$ when $\theta' = -\theta$	1
$\epsilon_2 = \epsilon_3$ or $\epsilon_2 \neq \epsilon_3$	$\{x\}$	$(q-1)/2$
$(\epsilon_1, \epsilon_1, \epsilon_2, \epsilon_2)$ split+quadratic	$\{x, -x, \theta\theta'/x, -\theta\theta'/x\}$ when $\theta' = -\theta$	1
$\epsilon_1 = \epsilon_2$ or $\epsilon_1 \neq \epsilon_2$	$\{x, \theta\theta'/x\}$	$(q-1)/2$
$(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_2)$ cubic $p \neq 3$	$\{x, \zeta_3 x, \zeta_3^2 x\}$ when $q \equiv 1 \mod 3$	2
$\epsilon_1 = \epsilon_2$ or $\epsilon_1 \neq \epsilon_2$	$\{x\}$ when $q \equiv 1 \mod 3$	$(q-1)/3$
	$\{x\}$ when $q \equiv -1 \mod 3$	$(q+1)/3$
$(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_2)$ cubic $p = 3$	$\{x\}$	$(q+3)/3$
$\epsilon_1 = \epsilon_2$ or $\epsilon_1 \neq \epsilon_2$		

□

Two explicit applications of Theorem 2.5.2 are below.

PROOF. $(\epsilon_1, \epsilon_1, \epsilon_2, \epsilon_2)$ split+quadratic with odd p:

Recall that $|\mathcal{N}_W| = p(q-1)^2(q^2-1)q^{E(\epsilon_1,\epsilon_1,\epsilon_2,\epsilon_2)}$. The sizes of the orbits are different depending on our choice of θ and θ'. In particular, if $\theta' = -\theta$, then $H = \{x, -x, \theta\theta'/x, -\theta\theta'/x\}$ and $|H| = 4$. In this case, the quadratic polynomial whose roots are θ and θ' must be of the form $f(x) = x^2 + B$ for $B \in k^*$ and $\gamma(x) = ax$ for $a \in k^*$, which means $f(\gamma(x)) = x^2 + B/a^2$. The number of irreducible polynomials of this type is equal to the number $(q-1)/2$ of choices for different constant terms, so there is one orbit in which $\theta' = -\theta$. Otherwise, $H = \{x, \theta\theta'/x\}$ and $|H| = 2$. There are $(q-1)/2$ other such orbits. The total weighted sum of covers is:

$$\frac{p(q-1)^2(q^2-1)q^{E(\epsilon_1,\epsilon_1,\epsilon_2,\epsilon_2)}}{p}\left(\frac{1}{4} + \frac{q-1}{2}\left(\frac{1}{2}\right)\right) = \frac{(q-1)^2(q^2-1)q^{E(\epsilon_1,\epsilon_1,\epsilon_2,\epsilon_2)+1}}{4}.$$

□

Proof. $(\epsilon_1, \epsilon_2, \epsilon_2, \epsilon_2)$ cubic with odd $p \neq 3$ and $q \equiv 1 \mod 3$:

Recall that $|\mathcal{N}_W| = p(q-1)(q^3-1)q^{E(\epsilon_1,\epsilon_2,\epsilon_2,\epsilon_2)}$. The sizes of the orbits are different depending on our choice of θ, θ' and θ''. In particular, if our polynomial is $f(x) = x^3 + C$ for $C \in k^*$, then $f(x)$ is fixed by $\gamma(x) = \zeta_3 x$, and there are $2(q-1)/3$ such irreducible polynomials. To determine how many of these are in the same orbit, note that if $\gamma(f(x)) = x^3 + D$ for $D \in k^*$, then $\gamma(x) = ax$ for $a \in k^*$, so $\gamma(f(x)) = x^3 + C/a^3$, meaning C can change by a cube. There are $(q-1)/3$ cubes, so by the Orbit-Stabilizer Theorem, there are two orbits in which $|H| = 3$. Otherwise, there are $(q+5)/3 - 2$ orbits in which $H = \{x\}$ and $|H| = 1$. The total weighted sum of covers is:

$$\frac{p(q-1)(q^3-1)q^{E(\epsilon_1,\epsilon_2,\epsilon_2,\epsilon_2)}}{p}\left(\frac{2}{3} + \left(\frac{q+5}{3} - 2\right)\right) = \frac{(q-1)(q^3-1)(q+1)q^{E(\epsilon_1,\epsilon_2,\epsilon_2,\epsilon_2)}}{3}.$$

□

CHAPTER 4

Applications

4.1. Previous Results: $p = 2$

Howe looked at the case in which $p = 2$ for genus $g = 1$.

Theorem 4.1.1. *[5, Corollary 2.2] As $[C]$ ranges over the k-isomorphism classes of Artin-Schreier covers C of genus 1, then the weighted count is*

$$\sum_{[C]} \frac{1}{|\mathrm{Aut}_k(C)|} = q.$$

In addition, [2] and [10] considered the cases in which $p = 2$ for genus $g = 2$ and genus $g = 3$. The results are summarized below for $g = 2$:

Theorem 4.1.2. *[2, Theorem 18] For $p = 2$ and $g = 2$, as $[C]$ ranges over the k-isomorphism classes of Artin-Schreier covers C of genus 2 defined over k, then*

$$\sum_{[C]} \frac{1}{|\mathrm{Aut}_k(C)|} = q^3.$$

Ramification Divisor	*Weighted Number of Covers*
$(1,1,1)$ *split*	$(q-1)^3/6$
$(1,1,1)$ *quadratic*	$(q-1)(q^2-1)/2$
$(1,1,1)$ *cubic*	$(q^3-1)/3$
$(1,3)$	$q(q-1)$
(5)	q

For the genus 3 case, [2] and [10] also have a table of weighted sums:

THEOREM 4.1.3. *[10, Theorem 8] For $p = 2$ and $g = 3$, as $[C]$ ranges over the k-isomorphism classes of Artin-Schreier covers C of genus 3, then*

$$\sum_{[C]} \frac{1}{|\mathrm{Aut}_k(C)|} = q^5.$$

Ramification Divisor	*Weighted Number of Covers*
$(1,1,1,1)$ *split*	$(q-2)(q-1)^4/24$
$(1,1,1,1)$ *split + quadratic*	$q(q+1)(q-1)^3/4$
$(1,1,1,1)$ *quadratic*	$(q^2-1)^2(q-2)/8$
$(1,1,1,1)$ *cubic*	$(q+1)(q-1)^2(q^2+q+1)/3$
$(1,1,1,1)$ *quartic*	$q(q^4-1)/4$
$(1,1,3)$ *split*	$q(q-1)^3/2$
$(1,1,3)$ *quadratic*	$q(q+1)(q-1)^2/2$
$(3,3)$ *split*	$q^2(q-1)/2$
$(3,3)$ *quadratic*	$q^2(q-1)/2$
$(1,5)$	$q^2(q-1)$
(7)	q^2

4.2. RESULTS FOR ODD p

4.2.1. DIMENSION. We note that the results of Pries and Zhu are applicable to the moduli space for these Artin-Schreier covers of genus $d(p-1)/2$ for $1 \leq d \leq 5$ [11]. In fact, the coefficients from the weighted counts give us information about the dimensions of the irreducible components of the moduli space for Artin-Schreier covers.

First, we state the results from Pries and Zhu:

THEOREM 4.2.2. *[11, Theorem 1.1] Let $\mathcal{AS}_{g,s}$ denote the moduli space of Artin-Schreier covers of genus g and p-rank s, where $g = d(p-1)/2$ for $d \geq 1$ and $s = r(p-1)$ for $r \geq 0$.*

(1) The set of irreducible components of $\mathcal{AS}_{g,s}$ is in bijection with the set of partition $\{e_1, e_2, \cdots, e_{r+1}\}$ of $d+2$ into $r+1$ positive integers such that each $e_j \not\equiv 1 \bmod p$.

(2) The irreducible components of $\mathcal{AS}_{g,s}$ for the partition $\{e_1, e_2, \cdots, e_{r+1}\}$ has dimension

$$d - 1 - \sum_{j=1}^{r+1} \lfloor (e_j - 1)/p \rfloor.$$

Note that using the notation from earlier, $\epsilon_j = e_j - 1$ here.

For arbitrary p and $g = d(p-1)/2$, it is known that the weighted sum of Artin-Schreier covers C of genus g defined over k. The leading coefficient of the weighted sum corresponds to the number of components, and the exponent of the leading term is the dimension of the components.

4.2.3. CASE $p = 3$. We give the results for $p = 3$.

THEOREM 4.2.4. *As $[C]$ ranges over the k-isomorphism classes of Artin-Schreier covers C of genus g, then the weighted count is*

$$\sum_{[C]} \frac{1}{|\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle \iota \rangle|} = \begin{cases} 1 & \text{if } g = 1 \\ q-1 & \text{if } g = 2 \\ q^2 & \text{if } g = 3 \\ 2q^3 - q^2 & \text{if } g = 4 \\ q^4 & \text{if } g = 5 \end{cases}$$

Details are found in the following table:

Genus	*Case*	*Dimension*	*Count*
1	*(2)*	*0*	*1*
2	*(1,1)*	*1*	$q-1$
3	*(1,2)*	*2*	q^2-q
	(4)	*1*	q
4	*(1,1,1)*	*3*	q^3-q^2
	(2,2)	*3*	q^3-q^2
	(5)	*2*	q^2
5	*(1,1,2)*	*4*	$q^4-2q^3+q^2$
	(1,4)	*3*	q^3-q^2
	(6)	*2*	q^2

Proof. The proof for each of these cases follows from Propositions 3.1.1, 3.2.2, and 3.2.11. □

4.2.5. Cases $p \geq 5$. In general, for odd $p \geq 5$ and $g = d(p-1)/2$ for $1 \leq d \leq 5$, we have the following:

THEOREM 4.2.6. *As $[C]$ ranges over the k-isomorphism classes of Artin-Schreier covers C of genus g, then the weighted count is*

$$\sum_{[C]} \frac{1}{|\mathrm{Cent}_{\mathrm{Aut}_k(C)}\langle\iota\rangle|} = \begin{cases} 1 & \text{if } g = 1(p-1)/2 \\ 2q-1 & \text{if } g = 2(p-1)/2 \\ 2q^2-q & \text{if } g = 3(p-1)/2 \\ 3q^3-3q^2 & \text{if } g = 4(p-1)/2, p = 5 \\ 4q^3-3q^2 & \text{if } g = 4(p-1)/2, p \geq 7 \\ 3q^4-3q^3+q^2 & \text{if } g = 5(p-1)/2, p = 5 \\ 4q^4-4q^3+q^2 & \text{if } g = 5(p-1)/2, p \geq 7 \end{cases}$$

Genus	*Case*	*Dimension*	*Count*
$1(p-1)/2$	*(2)*	*0*	*1*
$2(p-1)/2$	*(1,1)*	*1*	$q-1$
	(3)	*1*	q
$3(p-1)/2$	*(1,2)*	*2*	q^2-q
	(4)	*2*	q^2
$4(p-1)/2$	*(1,1,1)*	*3*	q^3-q^2
	(1,3)	*3*	q^3-q^2
	(2,2)	*3*	q^3-q^2
	(5)	*3*	q^3 *if* $p \geq 7$
$5(p-1)/2$	*(1,1,2)*	*4*	$q^4-2q^3+q^2$
	(1,4)	*4*	q^4-q^3
	(2,3)	*4*	q^4-q^3
	(6)	*3*	q^3 *if* $p=5$
		4	q^4 *if* $p \geq 7$

PROOF. The proof for each of these cases follows from Propositions 3.1.1, 3.2.2, and 3.2.11. □

CHAPTER 5

Future Work

We have yet to determine θ_H and H for the Quadratic and Quartic four-branch point cases, which would extend the results to $g = 6(p-1)/2$. Specifically, we want to find the W for which $\Gamma_W \neq \{\mathrm{id}\}$. This entails fixing $H \subset S_4$ and finding the number of orbits of W for which Γ_W is conjugate to H under $\mathrm{PGL}_2(k)$.

Similar methods used for the Split, Split+Quadratic, and Cubic cases may be insufficient for the Quadratic and Quartic cases. Some progress towards this is found below.

5.1. Quadratic Case

Recall from Section 3.2.9.2 that $W = \{\theta, \theta', \tau, \tau'\}$ where $\theta, \theta', \tau, \tau' \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. $\{\theta, \theta'\}$ and $\{\tau, \tau'\}$ are the pairs of roots for irreducible monic quadratic polynomials $f_1(x)$ and $f_2(x)$. Consider $f(x) = f_1(x)f_2(x)$ over $\mathbb{F}_q = k$. We had determined that the only possibilities for mappings to fix f_1 are:

$$\gamma_1 = \begin{pmatrix} a & cs \\ c & a \end{pmatrix} \text{ and } \gamma_2 = \begin{pmatrix} a & -cs \\ c & -a \end{pmatrix}$$

for $a, c \in k$ not both equal to 0. We attempt to understand the orbits better by closely examining γ_2.

In addition, there are also γ which swap f_1 and f_2, some of which could be order 2 or order 4.

In all of these cases, we find

$$\{f(x) = (x^2 - s)f_2 \mid \gamma \text{ fixes } f(x)\}$$

or the complete set of polynomials $f(x)$ with nontrivial stabilizer.

5.1.1. Elements of the Form γ_2. We compute:

$$\begin{aligned}(cx-a)^2 f_2\left(\frac{ax-cs}{cx-a}\right) &= x^2(a^2+Aac+Bc^2) - x(2acs+Aa^2+Ac^2s+2Bac) \\ &\quad +c^2s^2+Aacs+Ba^2 \\ &\stackrel{set}{=} \lambda(x^2+Ax+B)\end{aligned}$$

for some scaling factor $\lambda \in k^*$.

Equating the coefficients for the leading terms, we get $a^2+Aac+Bc^2=\lambda$. This gives the following two equations from the linear and constant terms:

$$\begin{aligned}2Aa^2+2acs+Ac^2s+2Bac+A^2ac+ABc^2 &= 0 \\ ABac+B^2c^2-c^2s^2-Aacs &= 0\end{aligned}$$

- $c=0$ means $\gamma_2(x)=-x$. Thus, $f_2=x^2+B$ where $B\neq -s$ and $B\neq 0$. The number of choices is $(q-1)/2-1=(q-3)/2$.
- Suppose $c\neq 0$. Without loss of generality, let $c=1$, and we have the conditions:

$$\begin{aligned}(2a+A)(Aa+B+s) &= 0 \\ (B-s)(Aa+B+s) &= 0\end{aligned}$$

  - Suppose $Aa+B+s\neq 0$. Then $B=s$ and $A=-2a$, so $f_2=x^2-2ax+s$. We need $4a^2-4s$ to be a nonsquare in k for this quadratic to be irreducible in k, or

$a^2 - s$ to be a nonsquare. Let

$$N = \#\{a \mid a^2 - s \text{ is not a square in } k\}.$$

We consider $N = q - M$ where

$$M = \#\{a \mid a^2 - s = t^2 \in k\}$$

and

$$M' = \#\{(a, t) \mid a^2 - t^2 = s\}.$$

Note that when $(a, t) \in M'$, then so is $(a, -t)$, so $M' = 2M$. Also, if $t = 0$, then $a^2 = s$ but s cannot be a square, so $t \neq 0$. Let $a^2 = z$ and $t^2 = w$. The exact same Gauss sum computation from Case 2 yields $M' = q - 1$, which implies that $M = (q - 1)/2$, so $N = (q + 1)/2$.

– Suppose $Aa + B + s = 0$. Then $B = -(Aa + s)$, so $f_2 = x^2 + Ax - (Aa + s)$. We want to count the number N of pairs (A, a) for $A, a \in k$ where $A^2 + 4Aa + 4s$ is not a square in k. We introduce a change of variables and let $D = A + 2a$ and $d = 2a$. Note there is a bijection between the pairs (A, a) and (D, d). Completing the square, we now want $D^2 - d^2 + 4s$ to not be a square in k. Thus, N is $q^2 - M$ where

$$M = \#\{(D, d) \mid D^2 - d^2 + 4s \text{ a square in } k\}$$

and

$$M' = \#\{(D, d, t) \mid D^2 - d^2 + 4s = t^2 \in k\}.$$

Suppose $t = 0$. Then we count

$$T = \#\{(D, d, 0) \mid D^2 - d^2 = -4s \in k\}.$$

Let $D^2 = z$ and $d^2 = w$ in k. We have

$$\begin{aligned}
T &= \sum_{z-w=-4s} \left(1 + \binom{z}{q}\right)\left(1 + \binom{w}{q}\right) \\
&= \sum_{z-w=-4s} \left(1 + \binom{z}{q} + \binom{w}{q} + \binom{z}{q}\binom{w}{q}\right) \\
&= \sum_{z-w=-4s} 1 + \sum_{z-w=-4s} \binom{z}{q} + \sum_{z-w=-4s} \binom{w}{q} + \sum_{z-w=4s} \binom{z}{q}\binom{w}{q} \\
&= q + 0 + 0 + \sum_{z-w=-4s} \binom{zw}{q} \\
&= q + \sum_{z-w=-4s, w\neq 0} \binom{z/w}{q} \\
&= q + \sum_{z\neq -4s} \binom{z/(z+4s)}{q}
\end{aligned}$$

Now let $y = z/(z + 4s)$. Solving for z, we get $z = -4sy/(y - 1)$. So we have:

$$\begin{aligned}
T &= q + \sum_{y\neq 1} \binom{y}{q} \\
&= q - \binom{1}{q} \\
&= q - 1
\end{aligned}$$

Note that the map from (D, d, t) to (D, d) is two-to-one except when $t = 0$, so $M' = 2(M - T) + T = 2M - T$.

Now we consider M' with a generalized Gauss sum by letting $D^2 = z, d^2 = w, t^2 = u$ in k:

$$\begin{aligned}
M' &= \sum_{z-w-u=-4s} \left(1+\binom{z}{q}\right)\left(1+\binom{w}{q}\right)\left(1+\binom{u}{q}\right) \\
&= \sum_{z-w-u=-4s} \left(1+\binom{z}{q}+\binom{w}{q}+\binom{u}{q}+\binom{wz}{q}+\binom{wu}{q}+\binom{zu}{q}+\binom{zwu}{q}\right) \\
&= q^2 + \sum_{z-w-u=-4s} \binom{zwu}{q} \\
&= q^2 + \chi_1\chi_2\chi_3(-4s)\chi(1)\chi(-1)\chi(-1)J(\chi_1,\chi_2,\chi_3) \text{ [6, Theorem 8.7.5]} \\
&= q^2 + \chi(-1)\chi(4)\chi(s)(-1)^{(q-1)/2}(-1)^{(q-1)/2}J(\chi,\chi,\chi) \\
&= q^2 + (-1)^{(q-1)/2}(-1)(-1)^{q-1}J(\chi,\chi,\chi) \\
&= q^2 + (-1)^{(q+1)/2}J(\chi,\chi,\chi) \\
&= q^2 + (-1)^{(3q-1)/2}\chi(-1)q \text{ [6, Proposition 8.6.1]} \\
&= q^2 + (-1)^{(2q-1)}q \\
&= q^2 - q
\end{aligned}$$

where χ are all quadratic characters, and J is a Jacobi sum. Therefore, $M = (q^2-1)/2$, and $N = (q^2+1)/2$.

5.1.2. Order 2 Elements. We also consider γ which swap f_1 and f_2, some of which could be order 2.

Consider

$$\gamma_3^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 = \begin{pmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{pmatrix}.$$

Since this is of order 2, then $ac + cd = ab + bd = 0$, which implies that $a = -d$. Note that the case in which $b = c = 0$ can be avoided because this is a subcase of the elements of type γ_2.

- Suppose $a = 0$. Without loss of generality, let $c = 1$, so

$$\gamma_3 = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$$

or $x \mapsto b/x$ for $b \neq s, -s, 0$. There are $q - 3$ such γ_3. We compute

$$\begin{aligned} (-x^2/s) f_1(\gamma_3) &= x^2 - b^2/s \\ &\stackrel{set}{=} x^2 + Ax + B \end{aligned}$$

which implies that $A = 0$ and $B = -b^2/s$. So $f_2 = x^2 - b^2/s$, which is irreducible. There are $q - 3$ such choices.

- Suppose $a \neq 0$. Without loss of generality, let $a = 1$. Then

$$\gamma_3 = \begin{pmatrix} 1 & b \\ c & -1 \end{pmatrix}.$$

The determinant must be nonzero, so $-1 - bc \neq 0$, or $bc \neq -1$. In addition, since γ_3 cannot be of the type γ_2, then $b \neq -cs$. There are no overlaps in these two conditions, so the number of possible γ_3 is $q^2 - q - (q - 1)$. We compute

$$\begin{aligned} (cx - 1)^2/(1 - sc^2) f_1(\gamma_3) &= x^2 + x\left(\frac{2b + 2sc}{1 - sc^2}\right) + \frac{b^2 - s}{1 - sc^2} \\ &\stackrel{set}{=} x^2 + Ax + B \end{aligned}$$

so

$$f_2 = x^2 + x\left(\frac{2b+2sc}{1-sc^2}\right) + \frac{b^2-s}{1-sc^2}$$

for $1 - sc^2 \neq 0$.

Altogether, there are $q^2 - q - 2 = (q+1)(q-2)$ possible γ_3 with fixed set of size 1 each.

5.1.3. Order 4 Elements. Other γ which swap f_1 and f_2 could be of order 4.

γ_4 must have the property that γ_4^2 is equivalent to γ_1 or γ_2 since the square of γ_4 must fix $f_1(x) = x^2 - s$.

- Suppose γ_4^2 is of type γ_1. Then $a^2 + bc = d^2 + bc$ must be true, and $b = sc$. These imply that $a = \pm d$ and $b = sc$. If $a = d$, then γ_4 already fixes f_1, which means it is not of order 4. Thus, $a = -d$ must be true. In addition, since the determinant is nonzero, then $a^2 + sc^2 \neq 0$. If $c = 0$, then the matrix is of type γ_2, which already fixes f_1, so $c \neq 0$. This is equivalent to

$$\gamma_4 = \begin{pmatrix} a & s \\ 1 & -a \end{pmatrix}$$

which has nonzero determinant, so $a^2 \neq -s$, which eliminates two choices of a when $q \equiv 1 \bmod 4$. Thus, we have the following number of choices for γ_4:

$$\begin{cases} q-2 & q \equiv 1 \bmod 4 \\ q & q \equiv -1 \bmod 4 \end{cases}$$

We compute:

$$\begin{aligned} (x-a)^2/(a^2-s) f_1(\gamma_4) &= x^2 + x\left(\frac{4as}{a^2-s}\right) + \frac{s^2-as}{a^2-s} \\ &\overset{set}{=} x^2 + Ax + B \end{aligned}$$

so

$$f_2 = x^2 + x\left(\frac{4as}{a^2 - s}\right) - s$$

for $a^2 - s \neq 0$.

- Suppose γ_4^2 is of type γ_2. Then $a^2 + bc = -bc - d^2$ and $sc = -b$ or $a^2 + d^2 = 2sc^2$ and $b = -sc$. Suppose $c = 0$, then $a \neq -d$, otherwise γ_4 would not be of order 4. Thus, $a = d$, and there are $q - 1$ such automorphisms. Suppose $c \neq 0$. Without loss of generality, let $c = 1$, so

$$\gamma_4 = \begin{pmatrix} a & -s \\ 1 & d \end{pmatrix}$$

which has nonzero determinant. This implies $a^2 + d^2 = 2s$. We can count the number of such possibilities P with a Gauss sum. Let $a^2 = z$ and $d^2 = w$. We count

$$\begin{aligned} P &= \sum_{z+w=2s} \left(1 + \binom{z}{q}\right)\left(1 + \binom{w}{q}\right) \\ &= q + \sum_{z+w=2s, w\neq 0} \binom{z/w}{q} \\ &= q + \sum_{z\neq 2s} \binom{z/(2s-z)}{q} \end{aligned}$$

Let $y = z/(2s - z)$. Solving for z, we get $z = 2sy/(y + 1)$, so our sum is now

$$\begin{aligned} P &= \sum_{y\neq -1} \binom{y}{q} \\ &= q - \binom{-1}{q} \\ &= q - (-1)^{(q+1)/2} \end{aligned}$$

or

$$\begin{cases} q-1 & q \equiv 1 \bmod 4 \\ q+1 & q \equiv -1 \bmod 4 \end{cases}$$

We compute:

$$\begin{aligned} (x+d)^2/(a^2+s)f_1(\gamma_4) &= x^2 + x\left(\frac{-2a+2ds}{a^2+s}\right) + \frac{s^2+sd^2}{a^2+s} \\ &\stackrel{set}{=} x^2 + Ax + B \end{aligned}$$

so

$$f_2 = x^2 + x\left(\frac{-2a+2ds}{a^2+s}\right) + \frac{s^2+sd^2}{a^2+s}$$

for $a^2 + s \neq 0$.

5.2. Quartic Case

Let $W = \{\theta, \theta', \theta'', \theta'''\}$ where $\theta, \theta', \theta'', \theta''' \in \mathbb{F}_{q^4} \backslash \mathbb{F}_{q^2}$. γ for which $\gamma(W) = W$ can be of order 2 or 4.

5.2.1. Order 2 Elements.

Suppose

$$\gamma^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 = \begin{pmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{pmatrix}.$$

Since this is of order 2, then $ac + cd = ab + bd = 0$, which implies that $a = -d$, so

$$\gamma = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}.$$

We consider a generic monic quartic polynomial and simplify by depressing the quartic to $f(x) = x^4 + Bx^2 + Cx + D$ for $B, C, D \in k$.

- Case 1: $a = 0$. We compute

$$\begin{aligned} \frac{x^4}{D} \cdot f(\gamma(x)) &= x^4 + \frac{Cb}{Dc}x^3 + \frac{Bb^2}{Dc^2}x^2 + \frac{b^4}{Dc^4} \\ &\stackrel{set}{=} x^4 + Bx^2 + Cx + D \end{aligned}$$

which yields the conditions

$$\begin{aligned} \frac{b^4}{Dc^4} &= D \\ \frac{Bb^2}{Dc^2} &= B \\ \frac{Cb}{Dc} &= 0 \end{aligned}$$

- Case 2: $a \neq 0$. Without loss of generality, let $a = 1$. We have

$$\begin{aligned} (cx-1)^4 \cdot f(\gamma(x)) &= x^4(1 + Bc^2 + Cc^3 + Dc^4) \\ &\quad + x^3(4b + 2Bbc^2 - 2Bc + Cbc^3 - 3Cc^2 - 4Dc^3) \\ &\quad + x^2(6b^2 + Bb^2c^2 - 4Bbc + B - 3Cbc^2 + 3Cc + 6Dc^2) \\ &\quad + x(4b^3 - 2Bb^2c + 2Bb + 3Cbc - C - 4Dc) + b^4 + Bb^2 - Cb + D \\ &\stackrel{set}{=} x^4 + Bx^2 + Cx + D \end{aligned}$$

which leads to some complicated conditions when we equate coefficients.

5.2.2. Order 4 Elements. Suppose

$$\gamma^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 = \begin{pmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{pmatrix}.$$

Since this is of order 4, then the square must be an order 2 matrix, so $a^2 + bc = -(bc + d^2)$, which implies that $a^2 + 2bc + d^2 = 0$. However, it is unclear how best to use this condition using similar approaches for the other cases.

BIBLIOGRAPHY

1. Bradley W. Brock and Andrew Granville, *More points than expected on curves over finite field extensions*, Finite Fields Appl. **7** (2001), no. 1, 70–91.
2. Gabriel Cardona, Enric Nart, and Jordi Pujolàs, *Curves of genus two over fields of even characteristic*, Mathematische Zeitschrift **250** (2005), no. 1, 177–201.
3. Gerard van der Geer and Marcel van der Vlugt, *Supersingular curves of genus* 2 *over finite fields of characteristic* 2, Mathematische Nachrichten **159** (1992), 73–81.
4. J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over a finite field*, Princeton Series in Applied Mathematics, Princeton University Press, Princeton, NJ, 2008.
5. Everett W. Howe, *On the group orders of elliptic curves over finite fields*, Compositio Math. **85** (1993), no. 2, 229–247.
6. Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.
7. Amparo López, Daniel Maisner, Enric Nart, and Xavier Xarles, *Orbits of Galois invariant n-sets of* $\mathbb{P}^1$ *under the action of* PGL_2, Finite Fields Appl. **8** (2002), no. 2, 193–206.
8. Amparo López and Enric Nart, *Classification of Goppa codes of genus zero*, J. Reine Angew. Math. **517** (1999), 131–144.
9. James S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980.
10. Enric Nart and Daniel Sadornil, *Hyperelliptic curves of genus three over finite fields of even characteristic*, Finite Fields and their Applications **10** (2004), no. 2, 198–220.
11. Rachel Pries and Hui June Zhu, *The p-rank stratification of Artin-Schreier curves*, Annales de l'Institut Fourier **61** (2012).

12. Henning Stichtenoth, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009.

13. D. C. van Leijenhorst, *Orbits on the projective line*, J. Combin. Theory Ser. A **31** (1981), no. 2, 146–154.

14. Kenneth S Williams, *Note on cubics over GF(2n) and GF(3n)*, Journal of Number Theory **7** (1975), no. 4, 361 – 365.