On Invariants of Artin-Schreier Curves

Juanita Duque-Rosero, Heidi Goodson, Elisa Lorenzo García, Beth Malmskog, and Renate Scheidler

Abstract The main goal of this article is to expand the theory of invariants of Artin-Schreier curves by giving a complete classification in genus 3 and 4. To achieve this goal, we first establish standard forms of Artin-Schreier curves and determine all isomorphisms between curves in this form. We then compute reconstructing systems of invariants for curves in each connected component of the strata of the moduli spaces for Artin-Schreier curves of genus 3 and 4 for $p > 2$.

2020 Mathematics Subject Classification 11G20 · 14L24 · 13A50 · 14D20 · 14D22 · 14G15 · 14H10 · 14H37 · 14H45 · 14Q05

J. Duque-Rosero (✉)
Department of Mathematics and Statistics, Boston University, Boston, MA, USA
e-mail: juanita@bu.edu
URL: https://juanitaduquer.github.io

H. Goodson
Department of Mathematics, Brooklyn College, Brooklyn, NY, USA
e-mail: heidi.goodson@brooklyn.cuny.edu
URL: https://sites.google.com/site/heidigoodson

E. Lorenzo García
Institut de Mathématiques, Université de Neuchâtel, Neuchâtel, Switzerland
Laboratoire IRMAR, Université de Rennes 1, Rennes Cedex, France
e-mail: elisa.lorenzo@unine.ch; elisa.lorenzogarcia@univ-rennes1.fr
URL: https://sites.google.com/site/elisalorenzo

B. Malmskog
Department of Mathematics and Computer Science, Colorado College, Colorado Springs, CO, USA
e-mail: bmalmskog@coloradocollege.edu
URL: https://malmskog.wordpress.com

R. Scheidler
Department of Mathematics and Statistics, University of Calgary, Calgary, AB, Canada
e-mail: rscheidl@ucalgary.ca
URL: https://cpsc.ucalgary.ca/ rscheidl

S. Akhtari et al. (eds.), *Research Directions in Number Theory*, Association for Women in Mathematics Series 39, https://doi.org/10.1007/978-3-032-11183-8_6

1 Introduction

Artin-Schreier theory derives from a 1927 paper of Emil Artin and Otto Schreier characterizing degree p Galois extensions of a field of characteristic p [AS27]. Artin and Schreier proved that such an extension $K(y)/K$ is precisely the splitting field of a polynomial in y of the form $y^p - y - \alpha$, where $\alpha \in K$ and $\alpha \neq \beta^p - \beta$ for any $\beta \in K$. Such extensions are now referred to as Artin-Schreier extensions, and the varieties defined by the associated polynomials are called Artin-Schreier curves. In this article, we aim to parameterize moduli spaces of Artin-Schreier curves in characteristic $p > 2$ by computing invariants of the curves.

It is well-known that elliptic curve isomorphism classes are given by the their j-invariants. In genus 2, we can describe isomorphism classes of curves using Igusa invariants [Igu60]. There are also examples of invariant computations in higher genus. For example, there are results for some genus 3 curves in [Shi67, Dix87, Ohn07], hyperelliptic curves in [LR12], Picard curves in [KLS20], Ciani curves in [BCK21], and others. In general, these calculations are done over the complex numbers, but they usually extend well to fields of large characteristic (genus 2 curves in [Liu93], genus 3 curves in [Bas15], [LLLR21, Sect. 4]). The sources [CFA06, Sect. 14.5] and [Liu02, Sect. 7.4.3] specifically cover Artin-Schreier curves in characteristic 2, which are hyperelliptic. However, there are still many cases missing from the literature, including "small cases" such as non-hyperelliptic curves of genus $g = 3$ in characteristic $p = 3$.

Artin-Schreier curves have undergone intense research not only as objects of mathematical interest in their own right, but also for their applications to coding theory (see [vdGvdV91] for example). For certain families of Artin-Scheier curves over a rational function field $K = \mathbb{F}_q(x)$, where q is a power of p, it is possible to provide point counts, find their automorphism groups, and determine their zeta functions [vdGvdV92, BHM16]. Such families frequently contain curves with many points, including maximal curves with respect to the Weil bound. Investigations of Artin-Schreier point counts from the perspective of arithmetic statistics can be found in [Ent12, BDF12, BDFL16].

In this paper, we compute invariants for Artin-Schreier curves of genus 3 and 4 in characteristic $p > 2$. Our work builds on that of Pries and Zhu, who determined the strata and dimensions of irreducible components of the moduli spaces of Artin-Schreier curves [PZ12]. We seek to characterize these moduli spaces concretely by parameterizing them via invariants. Our main ideas are taken from Geometric Invariant Theory (GIT), which was first developed by Mumford in 1965 [Mum65]. This theory provides techniques for forming the "quotient" of an algebraic variety (or scheme) X by a group G and is especially useful for constructing moduli spaces as quotients of schemes parameterizing objects. We provide an overview of invariant theory in Sect. 2.1 and of Artin-Schreier curves, their moduli spaces, and their isomorphisms in Sect. 2.2.

As in the genus 1 and 2 cases, it is useful to work with a standard form for Artin-Schreier curves in order to determine their invariants. Section 3 develops a standard

Table 1 Reconstructing invariants for all Artin-Schreier curves of genus $g = 3, 4$ in characteristic $p > 2$. The curves are classified by their p-rank s

g	p	s	Standard form	Set of reconstructing invariants over $\overline{\mathbb{F}}_p$
3	3	0	$y^3 - y = x^4 + ax^2$	$\{a^4\}$
3	3	2	$y^3 - y = x^2 + ax + \frac{b}{x}$	$\{a^4, ab, b^4\}$
3	7	0	$y^7 - y = x^2$	$\emptyset$
4	3	0	$y^3 - y = x^5 + cx^4 + dx^2$	$\{(c^3+d)^{10}, (-cd-\epsilon^2)^5, (c^3+d)^2(-cd-\epsilon^2)\}, \epsilon^3 = c$
4	3	2	$y^3 - y = x^2 + ax + \frac{b}{x} + \frac{c}{x^2}$	$\{c, ab, a^4c^2 - b^4\}$
4	3	4	$y^3 - y = x^2 + ax + \frac{b}{x} + \frac{c}{x-1}$	$\{(abc)^2, (abc)(a-b-c), ab+ac-bc\}$
4	5	0	$y^5 - y = x^3 + ax^2$	$\{a^{12}\}$
4	5	1	$y^5 - y = x + \frac{a}{x}$	$\{a^2\}$

Table 2 Partitions $\vec{E}$ of $D+2$ corresponding to the irreducible components of $\mathcal{AS}_{g,s}$ and the dimension of each irreducible component $\mathcal{AS}_{g,\vec{E}}$ for $g = 3, 4$ and $p \geq 3$

g	p	D	s	$\vec{E}$	dim $\mathcal{AS}_{g,\vec{E}}$
3	3	3	0	{5}	1
			2	{3, 2}	2
	7	1	0	{3}	0
4	3	4	0	{6}	2
			2	{3, 3}	3
			4	{2, 2, 2}	3
	5	2	0	{4}	1
			4	{2, 2}	1

form for Artin-Schreier curves. We also describe the isomorphisms between standard forms in this section. In Sect. 4, we determine reconstructing systems of invariants for all Artin-Schreier curves of genus 3 and 4 for primes $p > 2$, as listed in Table 2. This allows us to prove our main result, given in the following theorem.

Theorem 1.1 *A system of reconstructing invariants for all Artin-Schreier curves of genus $g = 3, 4$ in characteristic $p > 2$ is given in Table 1.*

For these curves, the strata and dimensions of the irreducible components of their moduli spaces are completely characterized in Table 2. The standard forms (see Theorem 3.3) and invariants listed in Table 1 are derived in the examples in Sect. 4.

The remainder of this paper is devoted to the proof of Theorem 1.1. We start by computing sets of invariants directly. We then show that these sets allow us to reconstruct standard forms of Artin-Schreier curves. Finally, standard invariant theoretic results summarized in Sect. 2 establish that these sets must generate the full invariant ring.

2 Background and Preliminaries

In this section we recall the basic definitions and results on invariant theory and Artin-Schreier curves that we will require for the work herein.

2.1 A Brief Introduction to Invariant Theory

Here we mainly follow [Bas15, DK02, DK08, Dol03, Eis95, Eis05]. The most important concepts in this section are the definitions of primary and secondary invariants. The main result is Corollary 2.13 that will allow us to manually compute generating sets of invariants in the examples we consider in this paper. For completeness we also introduce the concept of Hilbert series and how to compute them with the Molien-Weyl formula (see Theorem 2.6). This produces a second method for computing invariants that can be used to double-check our computations. Moreover, the algorithm implemented in Magma [BCP97] to compute invariants is also based on these ideas. Our computations in Sect. 4 can be corroborated by Magma.

Let K be an algebraically closed field. Let G be a linear algebraic group defined over K, acting on an algebraic variety G also defined over K. This action defines another action on $K[X]$ by $(g \cdot f)(x) = f(g^{-1} \cdot x)$ for all $x \in X$, $f \in K[X]$, and $g \in G$.

Definition 2.1 An element $f \in K[X]$ is an *invariant* for G if $g \cdot f = f$ for all $g \in G$. The algebra of invariants is $K[X]^G := \{f \in K[X] :\ g \cdot f = f, \forall g \in G\}$.

We especially consider here the case in which $X = V$ is a rational representation of G of finite degree, i.e., a linear representation of finite dimension such that the group morphism $G \to \mathrm{GL}(V)$ is also a morphism of varieties. The K-algebras $K[V]$ and $K[V]^G$ are naturally graded K-algebras.

In our situation, G will be finite. Since all finite groups are reductive, we can use the following result due to Emmy Noether [Noe26], here using the wording of [DK02].

Proposition 2.2 (Noether Normalization Lemma) *Let R be a finitely generated algebra over a Noetherian commutative ring K, and let G be a finite group acting on R by automorphisms fixing K elementwise. Then R^G is finitely generated as a K-algebra.*

Noether's result is a special case of the following.

Theorem 2.3 (Hilbert Finiteness Theorem) *If G is a reductive algebraic linear group and V is a rational representation of G of finite degree, then $K[V]^G$ is of finite type.*

Definition 2.4 Let $A = \oplus_{i \geq 0} A_i$ with $A_0 = K$ be a graded K-algebra. A set of homogeneous elements $\theta_1, \ldots, \theta_r \in A$ is a *homogeneous system of parameters* (HSOP) if the following hold.

- $\theta_1, \dots, \theta_r$ are algebraically independent over K,
- A is a $K[\theta_1, \dots, \theta_r]$-module of finite type, i.e., there exist $\eta_1, \dots, \eta_s \in A$ such that

$$A = \eta_1 K[\theta_1, \dots, \theta_r] + \cdots + \eta_s K[\theta_1, \dots, \theta_r].$$

When $A = K[V]^G$ and the η_i are homogeneous, the elements θ_i (resp. η_i) are the *primary (resp. secondary) invariants* of A.

The Noether Normalization Lemma (Proposition 2.2) implies that a graded algebra of finite type always admits an HSOP.

Definition 2.5 The *Hilbert series* of a graded K-algebra of finite type $A = \oplus_{i\geq 0} A_i$ with $A_0 = K$ is the power series

$$H(A, t) = \sum_{i=0}^{\infty} \dim_K(A_i) t^i.$$

If $A = \eta_1 K[\theta_1, \dots, \theta_r] + \cdots + \eta_s K[\theta_1, \dots, \theta_r]$, then

$$H(A, t) = \frac{\sum_{i=1}^{s} t^{e_i}}{(1 - t^{d_1})\dots(1 - t^{d_r})},$$

where d_i (resp. e_i) is the degree of θ_i (resp. η_i).

Theorem 2.6 (Molien-Weyl Formula, [DK02], Sect. 4.6.1) *The Hilbert series of a rational representation* (V, ρ) *of finite degree of a compact group* G *is*

$$H(K[V]^G, t) = \int_G \frac{1}{\det(\mathrm{Id} - \rho(g)t)} d\mu(g),$$

where $d\mu$ *is the Haar measure of* G.

Corollary 2.7 *If* G *is a finite group and* $\mathrm{char}(K)$ *does not divide* $|G|$, *then*

$$H(K[V]^G, t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(\mathrm{Id} - t \cdot g)}.$$

Lemma 2.8 (Noether, Fleischmann, Benson, Fogarty, [DK02], Corollary 3.8.4) *With the previous notation, if* $\mathrm{char}(K)$ *does not divide* $|G|$, *then there exists a set of generators of* $K[X]^G$, *all of degree smaller or equal than* $|G|$.

These results produce algorithms to compute primary and secondary invariants for actions of finite groups in the non-modular case (i.e., $\mathrm{char}(K) = p$ does not divide $|G|$). More precisely, see Algorithms 3.5.4 and 3.7.2 in [DK02]. Moreover, a version of these algorithms is implemented in Magma. They can be extended to work in the modular case as discussed in [DK02, Sects. 3.3 and 3.4.2]; specifically in Algorithm 3.7.5 in loc. cit. and in [DK08]. A general bound for the degree of the generators is given in [Sym11, Corollary 0.2]. Again, some versions of these algorithms are also implemented in Magma.

Definition 2.9 A subset $S \subseteq K[X]^G$ is said to be *separating* if it satisfies the following property. For any two points $x, y \in X$, if there exists an invariant $f \in K[X]^G$ with $f(x) \neq f(y)$, then there exists an element $g \in S$ with $g(x) \neq g(y)$.

Definition 2.10 Let $A \subseteq K[X]$ be a subalgebra of a polynomial ring of positive characteristic p. Then the algebra

$$\hat{A} = \{f \in K[X] : f^{p^r} \in A \text{ for some } r \in \mathbb{N}\} \subseteq K[X]$$

is the *purely inseparable closure* of A in $K[X]$.

Theorem 2.11 ([DK02], Theorem 2.3.15) *Let X be an affine variety and $G \subseteq \mathrm{Aut}(K[X])$ a subgroup of the automorphisms of the coordinate ring $K[X]$. Then there exists a finite separating set $S \subseteq K[X]^G$.*

Theorem 2.12 ([DK02], Theorem 2.3.12) *Let G be a finite group. Set $K = \overline{\mathbb{F}}_p$ and let V be a K-rational representation of G. Let $A \subseteq K[V]^G$ be a finitely generated, graded, separating subalgebra. Then $K[V]^G = \hat{\tilde{A}}$, the purely inseparable closure of the normalization of A.*

Corollary 2.13 *Let X be an affine variety over $K = \overline{\mathbb{F}}_p$ and let $G \subseteq \mathrm{Aut}(K[X])$ be a finite subgroup. There exists $A \subseteq K[X]^G$ generated by a finite number of invariants from which one can reconstruct a point on X from its values. Moreover, for any such A, one has $K[X]^G = \hat{\tilde{A}}$, the purely inseparable closure of the normalization of A.*

A set of invariants that allow reconstruction of a point as described in Corollary 2.13 is referred to as a *reconstructing system*.

2.2 Artin-Schreier Curves

Throughout, let p be a prime and $\overline{\mathbb{F}}_p$ an algebraically closed field of characteristic p. An *Artin-Schreier curve* is a curve over $\overline{\mathbb{F}}_p$ with an affine model of the form

$$C_f : y^p - y = f(x), \tag{2.1}$$

where $f(x) \in \overline{\mathbb{F}}_p(x)$ and $f(x) \neq z^p - z$ for any $z \in \overline{\mathbb{F}}_p(x)$. Let $r + 1$ (with $r \geq 0$) be the number of distinct poles of $f(x)$, and denote by d_i the order of the i-th pole of $f(x)$. By [Sti09, Lemma 3.7.7 (b)], or as we describe in the proof of Theorem 3.3, we can assume that no d_i is a multiple of p. To simplify formulae, set

$$e_i := d_i + 1 \qquad (1 \leq i \leq r + 1).$$

Then by [Sti09, Proposition 3.7.8 (d)], the genus of C_f is given by

$$g = \frac{p-1}{2}D, \quad \text{where} \quad D = -2 + \sum_{i=1}^{r+1} e_i. \tag{2.2}$$

The possible pole counts and orders for C_f thus correspond to partitions of $D+2$ into components e_i.

The *p-rank* of a smooth, irreducible, projective $\overline{\mathbb{F}}_p$-curve X is the integer s such that the cardinality of the p-torsion of its Jacobian, $\mathrm{Jac}(X)[p](\overline{\mathbb{F}}_p)$, is p^s. Then $0 \le s \le g$, and the Deuring-Shafarevich formula (see [Sub75] for a full discussion) implies that for an Artin-Schreier curve $X = C_f$, we have

$$s = r(p-1). \tag{2.3}$$

Thus, the p-rank of C_f depends simply on the number of poles of $f(x)$, not the poles themselves or their orders.

Let $\mathcal{AS}_g$ denote the moduli space of Artin-Schreier $\overline{\mathbb{F}}_p$-curves of genus g and $\mathcal{AS}_{g,s}$ the locus corresponding to Artin-Schreier $\overline{\mathbb{F}}_p$-curves of genus g with p-rank exactly s. The following theorem, due to Pries and Zhu [PZ12], characterizes the stratification of $\mathcal{AS}_g$ by p-rank.

Theorem 2.14 ([PZ12], Theorem 1.1) *Let $g = D(p-1)/2$ with $D \ge 1$ and $s = r(p-1)$ with $r \ge 0$.*

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

(2) The irreducible component $\mathcal{AS}_{g,\vec{E}}$ of $\mathcal{AS}_{g,s}$ for the partition $\vec{E} = \{e_1, \ldots, e_{r+1}\}$ has dimension

$$\dim \mathcal{AS}_{g,\vec{E}} = D - 1 - \sum_{j=1}^{r+1} \lfloor (e_j - 1)/p \rfloor. \tag{2.4}$$

So the irreducible components of the p-rank strata of the moduli space $\mathcal{AS}_g$ correspond to the different possibilities for the number of distinct poles of $f(x)$ and their orders, given the constraint in (2.2). Note that an irreducible component $\mathcal{C}$ of $\mathcal{AS}_{g,s}$ is not necessarily an irreducible component of $\mathcal{AS}_g$. It may be that $\mathcal{C}$ is open in some higher-dimensional irreducible component of $\mathcal{AS}_g$.

We compute the partitions corresponding to the irreducible components of $\mathcal{AS}_{g,s}$ for small g in Table 2. We omit $p = 2$, because all Artin-Schreier curves in this characteristic are hyperelliptic; as mentioned earlier, their invariants and moduli are already well understood.

We now consider the isomorphisms of Artin-Schreier curves.

Lemma 2.15 *Let C_f and $\widetilde{C}_{\tilde{f}}$ be isomorphic Artin-Schreier curves as given in* (2.1). *Assume that the function field isomorphism $\varphi : \overline{\mathbb{F}}_p(\tilde{C}) \to \overline{\mathbb{F}}_p(C)$ fixes the p-extension $\overline{\mathbb{F}}_p(C)/\overline{\mathbb{F}}_p(x)$. Then φ must be of the form*

$$(x, y) \mapsto \left(\frac{\alpha x + \beta}{\gamma x + \delta}, \lambda y + h(x)\right), \tag{2.5}$$

where $\alpha, \beta, \gamma, \delta \in \overline{\mathbb{F}}_p$ with $\alpha\delta - \beta\gamma \in \overline{\mathbb{F}}_p^{\times}$, $\lambda \in \mathbb{F}_p^{\times}$, and $h(x) \in \overline{\mathbb{F}}_p(x)$.

Proof The isomorphism φ is completely determined by its respective images $\tilde{x}$ and $\tilde{y}$ of x and y. By assumption, the degree p extension $\overline{\mathbb{F}}_p(C)/\overline{\mathbb{F}}_p(x)$ is fixed and $\tilde{x}$ is a function of x not dependent on y. This implies that φ must descend to an isomorphism of $\overline{\mathbb{F}}_p(x)$. Hence

$$\tilde{x} = \varphi(x) = \frac{\alpha x + \beta}{\gamma x + \delta},$$

where $\alpha, \beta, \gamma, \delta \in k$, and $\alpha\delta - \beta\gamma \in \overline{\mathbb{F}}_p^{\times}$. To determine the image of y under φ, we note that φ is invertible in $\overline{\mathbb{F}}_p(x)(y)$, so it must be of the form

$$\tilde{y} = \varphi(y) = \frac{A(x)y + B(x)}{C(x)y + D(x)},$$

where $A(x), B(x), C(x), D(x) \in \overline{\mathbb{F}}_p(x)$. By substituting $\tilde{x} = \frac{\alpha x+\beta}{\gamma x+\delta}$ into the equation of $\tilde{C}_{\tilde{f}}$ and comparing coefficients for $\tilde{y}$, we may assume that $A(x) = \lambda \in \overline{\mathbb{F}}_p^{\times}$, $C(x) = 0$, and $D(x) = 1$. □

Corollary 2.16 *Let C_f be an Artin-Schreier curve as given in* (2.1). *Assume that C_f is not birational to a curve of the form*

(1) $y^p - y = \frac{a}{x^p - x}$, with $a \in \overline{\mathbb{F}}_p$; or
(2) $y^p - y = \frac{1}{x^{\lambda}}$, with $\lambda \mid p + 1$; or
(3) $y^3 - y = \frac{i}{x(x-1)}$, with $i^2 = 2$.

Then all the isomorphisms of C_f are given by isomorphisms as in (2.5).

Proof By [VM80, Theorem 6], for C_f not birational to a curve of the form (1)–(3), the cover of $\overline{\mathbb{F}}_p(x)$ of degree p is unique, so we can apply Lemma 2.15 to derive the desired result. □

Remark 2.17 Henceforth, we will refer to curves that are birational to a curve of the form (1)–(3) in Corollary 2.16 as *exceptional*. These curves have genus $(p-1)^2$, $\frac{(p-1)(\lambda-1)}{2}$, and 2, respectively.

Remark 2.18 The exceptional curve in case (2) of Corollary 2.16 does not appear for the range of parameters considered in this article, so we do not examine it further. In addition, it is hyperelliptic, and invariants for curves of this type are known (see [LR12]).

Lemma 2.19 *Let C_f be an exceptional Artin-Schreier curve as given in* (2.1). *Then the automorphisms of C_f are those of type* (2.5) *preserving the curve model, together with the automorphisms*

(1) $\tau : \begin{cases} x \mapsto y \\ y \mapsto x \end{cases}$ *if* $y^p - y = \frac{a}{x^p - x}$, *with* $a \in \overline{\mathbb{F}}_p$;

(2) $\phi : \begin{cases} x \mapsto \epsilon x y^{-(p+1)/\lambda} & \text{if } y^p - y = x^\lambda, \text{ with } \lambda \mid p+1 \text{ and } \lambda < p+1; \\ y \mapsto 1/y & \text{where } \epsilon \text{ is a } \lambda\text{-root of } -1; \end{cases}$

(2') ϕ *in (2) and* $\begin{cases} x \mapsto x + a^p & \text{if } y^p - y = x^{p+1}, \text{ where } a^{p^2} = -a \text{ and} \\ y \mapsto y + ax + b & b^p - b = -a^{p+1}. \end{cases}$

Proof It is straightforward to see that the isomorphisms from Corollary 2.16 are also isomorphisms for exceptional curves. The extra function field automorphisms are described in [VM80, Theorem 7] and [Hen78] or in [HKT08, Proposition 11.30, Exercise A.9]. □

Remark 2.20 The automorphism groups of the different cases in Corollary 2.16 and Lemma 2.19 are a semi-direct product of an abelian p-group of order p^2 with a dihedral group of order $2(p-1)$, so with cardinality $2p^2(p-1)$, in case (1), an extension of a cyclic group of order λ in PGL(2,p) with $\lambda < p+1$, so of cardinality $\lambda|PGL(2,p)| = \lambda(p+1)p(p-1)$, in case (2), and $PGU(3,p^2)$ in case (2′) where $|PGU(3,p^2)| = (p^3+1)p^3(p^2-1)$. Finally, in case (3), the automorphism group is a extension of a cyclic group of order 2 by S_4.

2.3 Fractional Linear Transformations Acting on $\overline{\mathbb{F}}_p(x)$

Let

$$\varphi(x,y) = \left(\frac{\alpha x + \beta}{\gamma x + \delta}, \lambda y + h(x)\right),$$

with $\alpha, \beta, \gamma, \delta, \lambda, h(x)$ as given in Corollary 2.16. For ease of exposition, define

$$M := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\overline{\mathbb{F}}_p) \text{ and } M(x) := \frac{\alpha x + \beta}{\gamma x + \delta}.$$

Let $f(x) \in \overline{\mathbb{F}}_p(x)$. The map $x \mapsto M(x)$ extends to an action of $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ on $\overline{\mathbb{F}}_p(x)$ by the extension $M(f(x)) = f(M(x))$, which induces an action on the projective line $\mathbb{P}^1(\overline{\mathbb{F}}_p)$ via the poles of functions in $\overline{\mathbb{F}}_p(x)$. When we consider functions with a single pole, this action is the inverse of the well-known action of Möbius transformations on $\mathbb{P}^1(\overline{\mathbb{F}}_p)$. For example, consider $f(x) = \frac{1}{x}$, a function with a single pole at $x = 0$. Then $f(M(x)) = \frac{\gamma x+\delta}{\alpha x+\beta}$, which has a pole at $x = \frac{-\beta}{\alpha}$ when $\alpha \neq 0$, and a pole at ∞ otherwise. The standard Möbius transformation of $\mathbb{P}^1(\overline{\mathbb{F}}_p)$ associated to M satisfies $M(0) = \frac{\beta}{\delta}$ if $\delta \neq 0$, with $M(0) = \infty$ when $\delta = 0$. However, $M^{-1}(0) = \frac{-\beta}{\alpha}$ when $\alpha \neq 0$, ∞ when $\alpha = 0$.

To avoid confusion with these actions, we set the following notation to view poles of functions as points in $\mathbb{P}^1(\overline{\mathbb{F}}_p)$ for the remainder of the paper. Let $P_\infty \in \mathbb{P}^1(\overline{\mathbb{F}}_p)$ be the pole of the function $x \in \overline{\mathbb{F}}_p(x)$. For $\mu \in \overline{\mathbb{F}}_p$, let $P_\mu \in \mathbb{P}^1(\overline{\mathbb{F}}_p)$ be the pole of the function $\frac{1}{x-\mu} \in \overline{\mathbb{F}}_p(x)$. Throughout, we will describe the action of $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ on poles using this notation. For later convenience, we describe the action of M on poles explicitly.

Lemma 2.21 *The transformation $M(x) = \frac{\alpha x+\beta}{\gamma x+\delta}$ sends the pole P_μ to $P_{\mu'}$, where $\mu' = M^{-1}(\mu) = \frac{\delta\mu-\beta}{-\gamma\mu+\alpha}$.*

3 Standard Form

Every Artin-Schreier curve C_f as given in (2.1) can be transformed into an isomorphic curve in *standard form*. While this form is not unique, there are a finite number of standard forms for a given isomorphism class, so this form facilitates our invariant computations. Informally, the idea is to find an isomorphism that sends the poles of C_f with the three highest (not necessarily distinct) orders to the pole P_∞ at infinity and the poles P_0 and P_1 at $x = 0$ and $x = 1$, respectively. In case C_f has at most two poles, they are sent to P_∞ and P_0 (for two poles) or simply to P_∞ (for only one pole), and certain normalizations are applied to the polynomial part on the right-hand side of (2.1).

The single pole case is the most complicated. Here, the unique pole is moved to infinity, so the right-hand side of C_f becomes a polynomial $f(x) \in \overline{\mathbb{F}}_p[x]$ of degree d, the order of the pole. We address this case in the following lemma.

Lemma 3.1 *Let C_f be an Artin-Schreier $\overline{\mathbb{F}}_p$-curve as given in (2.1) with a unique pole at infinity, where $f(x) \in \overline{\mathbb{F}}_p[x]$ is monic of degree $d > 1$. Then C_f is isomorphic to a curve of the form $C_g : y^p - y = g(x)$ with*

$$g(x) = x^d + \sum_{i=0}^{d-1} b_i x^i \in \overline{\mathbb{F}}_p[x],$$

where $b_i = 0$ whenever p divides i and $b_1 = 0$.

Proof We explicitly determine $\beta \in \overline{\mathbb{F}}_p$ and $h(x) \in \overline{\mathbb{F}}_p[x]$ such that the isomorphism $(x, y) \mapsto (x + \beta, y + h(x))$ transforms C_f into the required form.

Write

$$f(x) = a_d x^d + \sum_{i=0}^{d-1} a_i x^i$$

with $a_i \in \overline{\mathbb{F}}_p$ for $0 \le i \le d-1$ and $a_d = 1$. For any $\beta \in \overline{\mathbb{F}}_p$ we define

$$u_i(\beta) := \sum_{j=i}^{d} a_j \binom{j}{i} \beta^{j-i} \ (0 \le i \le d),$$

so $f(x+\beta) = \sum_{i=0}^{d} u_i(\beta)x^i$ and $u_i(0) = a_i$ for $0 \le i \le d$. Set $M = \lfloor d/p \rfloor$ and $m = \lfloor M/p \rfloor$, where $\lfloor \cdot \rfloor$ denotes the floor function. Then $Mp < d$, as p does not divide d. If $M > 0$, recursively define elements $b_i(\beta) \in \overline{\mathbb{F}}_p$ via

$$b_i(\beta)^p = \begin{cases} u_{ip}(\beta) & \text{for } M \ge i \ge m+1, \\ u_{ip}(\beta) + b_{ip}(\beta) & \text{for } m \ge i \ge 1. \end{cases}$$

Since $i < ip \le mp \le M$ for $1 \le i \le m$, the quantities $b_i(\beta)$ are well defined. Also define $b_0(\beta) \in \overline{\mathbb{F}}_p$ via the identity

$$b_0(\beta)^p - b_0(\beta) = u_0(\beta).$$

Let $f'(x)$ denote the formal derivative of $f(x)$ with respect to x. Since p does not divide d, the degree of $f'(x)$ is $d-1 > 0$, and we note that $u_1(\beta) = f'(\beta)$.

Now choose $\beta \in \overline{\mathbb{F}}_p$ such that $u_1(\beta) + b_1(\beta) = 0$. For this choice of β, define

$$h(x) = \sum_{i=0}^{M} b_i(\beta)x^i.$$

Then the isomorphism $(x, y) \mapsto (x+\beta, y+h(x))$ maps C_f to a curve of the form $C_g : y^p - y = g(x)$ where

$$g(x) = f(x+\beta) - h(x)^p + h(x) \in \overline{\mathbb{F}}_p[x].$$

Since $h(x)^p$ has degree $Mp < d$ and $f(x+\beta)$ is monic of degree d, $g(x)$ is also monic of degree d. It remains to show that the coefficients of $g(x)$ satisfy the desired conditions.

Every monomial of the form x^{ip} potentially appearing in $g(x)$ satisfies $0 \le i \le M$. For $i \ge 1$, the corresponding coefficient of $g(x)$ is

$$b_{ip}(\beta) = \begin{cases} u_{ip}(\beta) - b_i(\beta)^p & \text{for } M \ge i \ge m+1, \\ u_{ip}(\beta) - b_i(\beta)^p + b_{ip}(\beta) & \text{for } m \ge i \ge 1. \end{cases}$$

Moreover, $b_0(\beta) = u_0(\beta) - b_0(\beta)^p + \beta_0(\beta)$. By the definition of $b_i(\beta)$, we have $b_{ip} = 0$ for $0 \le i \le M$. Finally, the coefficient of x in $g(x)$ is $b_1(\beta) = u_1(\beta) + b_1(\beta)$, which also vanishes by our choice of β. □

Remark 3.2 The normalization conditions proposed in [Far10, Proposition 2.1.1] require the removal of the monomial x^{d-1} as well as all p-th power monomials in $f(x)$ via an iterative sequence of suitable isomorphisms. One difficulty arising with these restrictions is that in the case where $d \equiv 1 \pmod{p}$, removal of p-th powers already eliminates the monomial x^{d-1}, in which case it is desirable to remove a second coefficient in order to further simplify the curve model. It is in fact always possible to eliminate at least one of the next two highest order monomials x^{d-2}, x^{d-3}, but the form of the initial curve determines which of them can be removed. Specifically, all linear transformations on x leave the coefficient of x^{d-2} in $f(x)$ fixed, so this monomial can be eliminated precisely when the corresponding term in the initial curve vanishes. In order to avoid this dependence on the shape of the curve, we opt instead to remove the linear term and all p-th power monomials from $f(x)$ at once, with a single isomorphism. This choice of normalization has the advantage of being more canonical and thus mathematically more satisfying. However, in practice, it may come at the expense of complicating the calculation of the curve invariants compared to a model with fewer high degree monomials; the example in Sect. 4.3.1 illustrates this.

We now have all the ingredients to convert an Artin-Schreier curve to standard form.

Theorem 3.3 *Let p be an odd prime and C_f an Artin-Schreier $\overline{\mathbb{F}}_p$-curve as given in (2.1) with $r+1$ poles of respective orders $d_1 \ge d_2 \ge \ldots \ge d_{r+1}$. Then C_f is isomorphic to an Artin-Schreier curve*

$$C_g : y^p - y = g(x),$$

where $g(x) \in \overline{\mathbb{F}}_p(x)$ takes on one of the following forms:

(1) ***Case*** $r = 0$*:*

$$g(x) = x^{d_1} + Q(x)$$

where $Q(x) \in \overline{\mathbb{F}}_p[x]$ is a multiple of x^2 and no monomial appearing in $Q(x)$ has an exponent that is divisible by p.

(2) ***Case*** $r = 1$*:*

$$g(x) = F(x) + G\left(\frac{1}{x}\right),$$

where $F(x), G(x) \in \overline{\mathbb{F}}_p[x]$, $F(x)$ is monic, $\deg(F) = d_1$, $\deg(G) = d_2$*, and no monomial appearing in $F(x)$ or $G(x)$ has an exponent that is divisible by p.*

(3) ***Case*** *$r \geq 2$:*

$$g(x) = F(x) + G\left(\frac{1}{x}\right) + H\left(\frac{1}{x-1}\right) + S(x),$$

where $F(x), G(x), H(x) \in \overline{\mathbb{F}}_p[x]$, $\deg(F) = d_1$, $\deg(G) = d_2$, $\deg(H) = d_3$, *either* $S(x) = 0$ *or*

$$S(x) = \sum_{i=4}^{r+1} \frac{g_i(x - \lambda_i)}{(x - \lambda_i)^{d_i}},$$

with $\lambda_i \in \overline{\mathbb{F}}_p \backslash \{0, 1\}$, $g_i(x) \in \overline{\mathbb{F}}_p[x]$ *non-zero,* $\deg(g_i) < d_i$, *and no monomial appearing in* $F(x)$, $G(x)$, $H(x)$, *or any of the polynomials* $x^{d_i} g_i(x^{-1})$ *has an exponent that is divisible by* p, *for* $4 \leq i \leq r + 1$.

The curve C_g *is said to be in* standard form.

Proof We represent fractional linear transformations $M(x) = \dfrac{\alpha x + \beta}{\gamma x + \delta}$ by $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ as in Sect. 2.3.

We begin with the case $r = 0$, so C_f has a unique pole P_{μ_1} of order d_1. If $\mu_1 \neq \infty$, then $\mu_1 \in \overline{\mathbb{F}}_p$ and $f(x)$ is of the form

$$f(x) = \frac{f_\infty(x - \mu_1)}{(x - \mu_1)^{d_1}},$$

where $f_\infty(x) \in \overline{\mathbb{F}}_p[x]$ is non-zero of degree less than d_1. The matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{if } \mu_1 = \infty,$$

$$\begin{pmatrix} \mu_1 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{if } \mu_1 \in \overline{\mathbb{F}}_p,$$

send P_{μ_1} to P_∞, so we produce a curve of the form $y^p - y = \tilde{f}(x)$, where $\tilde{f}(x) \in \overline{\mathbb{F}}_p[x]$ is a polynomial of degree d_1. Let a be the leading coefficient of $\tilde{f}$. Applying a matrix of the form $\begin{pmatrix} a^{-1/p} & 0 \\ 0 & 1 \end{pmatrix}$ yields the curve $y^p - y = \tilde{g}(x)$ where $\tilde{g}(x) = \tilde{f}(a^{-1/d}x)$ is monic of degree d_1.

If $d_1 = 1$, then define $\gamma \in \overline{\mathbb{F}}_p$ via $\gamma^p - \gamma = \tilde{g}(0)$, the constant coefficient of $\tilde{g}(x)$. Then the isomorphism $(x, y) \mapsto (x, y + \gamma)$ produces the curve $y^p - y = x = x^{d_1}$. If $d_1 > 1$, then the isomorphism of Lemma 3.1 produces a curve C_g of the required form.

For the remaining cases (i.e., $r \geq 1$), the conversion of C_f to standard form is more easily done in two stages. The first stage applies a suitable fractional linear transformation of x to C_f that moves the highest order poles as explained earlier.

This is followed by a second sequence of linear transformations applied to y that eliminates p-th powers of x one-by-one.

Assume first that $r = 1$, so C_f contains two poles P_{μ_1}, P_{μ_2} of respective orders $d_1 \geq d_2$. Then the matrices

$$\begin{pmatrix} 1 & \mu_2 \\ 0 & 1 \end{pmatrix} \text{ if } \mu_1 = \infty \text{ and } \mu_2 \in \overline{\mathbb{F}}_p,$$
$$\begin{pmatrix} \mu_1 & 1 \\ 1 & 0 \end{pmatrix} \text{ if } \mu_1 \in \overline{\mathbb{F}}_p \text{ and } \mu_2 = \infty,$$
$$\begin{pmatrix} \mu_1 & \mu_2 \\ 1 & 1 \end{pmatrix} \text{ if } \mu_1 \in \overline{\mathbb{F}}_p \text{ and } \mu_2 \in \overline{\mathbb{F}}_p,$$

send P_1 and P_2 to P_∞ and P_0, respectively, and thus produce a curve of the form $y_p - y = \tilde{f}(x)$, where $\tilde{f}(x) \in \overline{\mathbb{F}}_p[x, x^{-1}]$ is a Laurent polynomial of degree d_1 in x and degree d_2 in x^{-1}. Let a be the coefficient of x^{d_1} in $\tilde{f}(x)$. As in the case $r = 0$, a scaling matrix of the form

$$\begin{pmatrix} a^{-1/p} & 0 \\ 0 & 1 \end{pmatrix}$$

yields an isomorphic curve $C_{\tilde{g}}$ where $\tilde{g}(x)$ is monic with respect to x.

The case $r = 2$ proceeds similarly. Suppose C_f has three or more poles. Let $P_{\mu_1}, P_{\mu_2}, P_{\mu_3}$ be poles of the three largest respective orders $d_1 \geq d_2 \geq d_3$. Then the matrices

$$\begin{pmatrix} \mu_3 - \mu_2 & \mu_2 \\ 0 & 1 \end{pmatrix} \quad \text{if } \mu_1 = \infty, \mu_2 \in \overline{\mathbb{F}}_p \text{ and } \mu_3 \in \overline{\mathbb{F}}_p,$$
$$\begin{pmatrix} \mu_1 & \mu_1 - \mu_3 \\ 1 & 0 \end{pmatrix} \quad \text{if } \mu_1 \in \overline{\mathbb{F}}_p, \mu_2 = \infty \text{ and } \mu_3 \in \overline{\mathbb{F}}_p,$$
$$\begin{pmatrix} -\mu_1 & \mu_2 \\ -1 & 1 \end{pmatrix} \quad \text{if } \mu_1 \in \overline{\mathbb{F}}_p, \mu_2 \in \overline{\mathbb{F}}_p \text{ and } \mu_3 = \infty,$$
$$\begin{pmatrix} \mu_1(\mu_3 - \mu_2) & \mu_2(\mu_1 - \mu_3) \\ \mu_3 - \mu_2 & \mu_1 - \mu_3 \end{pmatrix} \quad \text{if } \mu_i \in \overline{\mathbb{F}}_p \text{ for } i = 1, 2, 3,$$

send P_1, P_2, and P_3 to P_∞, P_0, and P_1, respectively. The same scaling matrix as in the case $r = 1$ produces a rational function $\tilde{g}(x)$ of the specified form that is monic in x.

Next, in both of the cases $r = 1$ and $r \geq 2$, we remove all the monomials of the form x^{kp} for $k \in \mathbb{Z} \setminus \{0\}$. The constant coefficient of $\tilde{g}(x)$ is handled separately at the end.

As described in [Far10, Proposition 2.1.1] and the subsequent discussion, removal of the monomials x^{kp} with $k > 0$ from $\tilde{g}(x)$ is accomplished iteratively via suitable translations of y, leaving x fixed. Suppose $\tilde{g}(x)$ contains a term of the form bx^{pk}, where $b \in \overline{\mathbb{F}}_p^\times$ and $1 \leq k \leq d_1 - 1$. Then the isomorphism $(x, y) \mapsto (x, y + b^{1/p}x^k)$

produces the curve $y^p - y = \tilde{g}(x) - bx^{kp} - e^{1/p}x^k$, where the term bx^{pk} no longer appears on the right-hand side. Systematically applying a finite number of suitable isomorphisms of this form, looping over the values of k in decreasing order from $k = \lfloor d_1/p \rfloor$ to $k = 1$, eliminates all monomials x^{kp} with $k > 0$. An analogous process, looping over all k from $-\lfloor (d_2 - 1)/p \rfloor$ to -1, eliminates all monomials x^{kp} with $k < 0$.

When $r = 1$, this process removes all monomials that are positive p-powers. So suppose that $r \geq 2$. Then for each pole P_μ with $\mu = 1$ or $\mu = \lambda_i$ $(4 \leq i \leq r + 1)$, we apply the isomorphisms $(x, y) \mapsto (x, y + b(x - \mu)^{-kp})$, where k runs from $-\lfloor (d_i - 1)/p \rfloor$ to -1 for $3 \leq i \leq r + 1$, to remove all terms involving powers $(x - \mu)^{kp}$ with $k < 0$.

We are at last left with a curve of the form $y^p - y = \tilde{g}(x)$, where no terms x^{pk} and $(x - \mu)^{-kp}$ for any pole $P_\mu \neq P_\infty$, with $k > 0$, appear in $\tilde{g}(x)$. It remains to eliminate the constant term $\tilde{g}(0)$. To that end, let $\gamma \in \overline{\mathbb{F}}_p$ such that $\gamma^p - \gamma = \tilde{g}(0)$. Then the isomorphism $(x, y) \mapsto (x, y + \gamma)$ yields the curve $y^p - y = g(x)$, where $g(x) = \tilde{g}(x) - \tilde{g}(0)$ is of the desired form. □

As mentioned above, the standard form of an Artin-Schreier curve is not unique. For example, the two standard form curves $y^3 - y = x^4 - x^2$ and $y^3 - y = x^4 + x^2$ are $\overline{\mathbb{F}}_3$-isomorphic via the isomorphism $(x, y) \mapsto (\sqrt{2}x, y)$; this is a special case of Proposition 4.1. However, for any non-exceptional curve, we see that the number of possible standard forms is finite and that the forms are easy to enumerate. In fact, the number of variable coefficients in each standard form is equal to the dimension of the component of the moduli space with the corresponding partition as described in Theorem 2.4.

In the next section, we discuss isomorphisms between Artin-Schreier curves in standard form.

3.1 Isomorphisms Between Curves in Standard Form

If we consider only Artin-Schreier curves in standard form, outside of the exceptional curves in Corollary 2.16, this narrows the possibilities for isomorphisms between them. Let

$$\varphi(x, y) = (M(x), \lambda y + h(x)), \tag{3.1}$$

with M, λ, $h(x)$ as in Corollary 2.16.

Lemma 3.4 *Let C_f and $C_{\tilde{f}}$ be isomorphic Artin-Schreier curves in standard form. Then for every choice of $M \in \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ for an isomorphism $\varphi(x, y)$ as in (3.1) between these curves, there is a unique choice of $h(x)$ up to a constant in $\mathbb{F}_p$; that is, up to (multiple) composition with the isomorphism $\sigma : (x, y) \mapsto (x, y + 1)$.*

Proof We apply φ to the equation $y^p - y = f(x)$ to obtain $f(x) = \frac{1}{\lambda}(f(M(x)) - h^p(x) + h(x))$. This enforces a unique choice of $h(x)$ up to a constant in $\mathbb{F}_p$. □

For $M \in \mathrm{GL}_2(\overline{\mathbb{F}}_p)$, we define $h_M(x) \in \overline{\mathbb{F}}_p(x)$ to be a choice of polynomial from Lemma 3.4, up to composition with powers of σ. An isomorphism between standard forms is then determined, up to composition with powers of σ, by the choice of $M \in GL_2(\overline{\mathbb{F}}_p)$ and $\lambda \in \mathbb{F}_p^\times$. Thus we may without confusion define

$$\varphi_{\lambda,M}(x, y) = (M(x), \lambda y + h_M(x)). \tag{3.2}$$

In our application, we consider rational functions $f(x)$ which appear in the standard form of curves $y^p - y = f(x)$ corresponding to a given prime p and partition $\vec{E} = \{e_1, e_2, \ldots, e_{r+1}\}$ of $D + 2$. As before, we assume that $e_{i+1} \le e_i$ for $1 \le i \le r$, where $d_i = e_i - 1$ for each i. Since genus and p-rank are invariant under isomorphism, isomorphic curves must correspond to the same partition $\vec{E}$. The isomorphism from one curve to another preserves the orders of distinct poles, but may change their locations.

The possible isomorphisms between non-exceptional Artin-Schreier curves in standard form can be determined by finding all $M \in \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ and $\lambda \in \mathbb{F}_p^\times$ that preserve all the restrictions on poles and curve coefficients imposed by Theorem 3.3 as well as the partition $\vec{E}$. In particular, subject to these conditions, subsets of poles may be permuted and curve coefficients changed by such an isomorphism. We designed standard forms in such a way that the number of free coefficients of $f(x)$ in the right-hand side of a standard form curve (2.1) is equal to the dimension d of the corresponding irreducible component of $\mathcal{AS}_{g,s}$. Thus, the group G of isomorphisms between standard forms must be finite, and we are able to completely enumerate the images of non-exceptional curves under G. Let $a_1, a_2, \ldots, a_d$ be the free coefficients of the standard form of some irreducible component. We can think of $\overline{\mathbb{F}}_p[a_1, a_2, \ldots, a_d]$ as the space containing all standard form models of curves in $\mathcal{AS}_{g,s}$. The isomorphisms in G act on $\overline{\mathbb{F}}_p[a_1, a_2, \ldots, a_d]$, and we seek a separating, or ideally, a reconstructing subset of the invariant ring $\overline{\mathbb{F}}_p[a_1, a_2, \ldots, a_d]^G$. Finding a minimal reconstructing set of invariants allows us to essentially parameterize an irreducible component of $\mathcal{AS}_{g,s}$.

Remark 3.5 As just mentioned, the number of free coefficients of a standard form is equal to the dimension of the corresponding irreducible component of $\mathcal{AS}_{g,s}$. This number is also equal to the number of primary invariants for the action of the finite group G acting on the coefficients of the standard form.

3.2 Standard Forms of Exceptional Curves

In Corollary 2.16 we described the isomorphisms from an Artin-Schreier curve C when the function field $\overline{\mathbb{F}}_p(C)$ has a single index p subextension associated to a genus 0 curve. Such a subextension gives a model of the curve of the form $y^p - y = f(x)$ and we discussed its standard forms in Sect. 3.1. We now investigate what standard forms can arise for the cases in which such an index p subextension is not unique. For each order p automorphism σ of C such that the quotient curve $C/\langle\sigma\rangle$ has genus 0, the degree p extension $\overline{\mathbb{F}}_p(C)/\overline{\mathbb{F}}_p(C/\langle\sigma\rangle)$ produces a way to write C as $y^p - y = f(x)$ where $y \in \overline{\mathbb{F}}_p(C)\backslash\overline{\mathbb{F}}_p(C/\langle\sigma\rangle)$ and $f(x) \in \overline{\mathbb{F}}_p(C/\langle\sigma\rangle)$.

Lemma 3.6 *Let $C : y^p - y = \frac{a}{x^p - x}$ be a curve as given in case (2.16) of Corollary 2.16. Then any standard form of C can be obtained by applying an isomorphism of the form in (2.5) through the procedure in Theorem 3.3 from the given model of C.*

Proof The automorphism group of C is isomorphic to $((C_p \times C_p) \rtimes C_{p-1}) \rtimes C_2$, generated by

$$\begin{aligned}
&(1, 0, 0, 0)(x, y) = (x + 1, y),\\
&(0, 1, 0, 0)(x, y) = (x, y + 1),\\
&(0, 0, 1, 0)(x, y) = (\mu x, y/\mu) \ \text{ with } \mu \in \overline{\mathbb{F}}_p^\times \text{ and}\\
&(0, 0, 0, 1)(x, y) = (y, x).
\end{aligned}$$

Any subgroup of order p consists of elements of the form $(\alpha, \beta, 0, 0)$ and is generated by an automorphism of the form $(0, 1, 0, 0)$ or $(1, \beta, 0, 0)$. The first of these does not change the curve equation. The second one produces a degree p extension $\overline{\mathbb{F}}_p(x, y)/\overline{\mathbb{F}}_p(y - \beta x, y^p - y)$ that is isomorphic to $\overline{\mathbb{F}}_p(\mathbb{P}^1)$ if $\beta = 0$; if $\beta \neq 0$, it defines the hyperelliptic curve of genus $p - 1$ given by $v^p - v = \frac{a}{u} - \beta u$. So once again we obtain the original equation $x^p - x = \frac{a}{y^p - y}$ and the result holds. □

A result from [Kon09] explicitly describes the isomorphism classes of these curves in terms of the non-standard model.

Lemma 3.7 ([Kon09, Lemma 3.1]) *Let $a, a' \in \overline{\mathbb{F}}_p^\times$. Then $y^p - y = \frac{a}{x^p - x}$ is isomorphic to $y^p - y = \frac{a'}{x^p - x}$ if and only if $a = \lambda a'$ for some $\lambda \in \mathbb{F}_p^\times$.*

Lemma 3.8 *Let $C : y^p - y = \frac{1}{x^\lambda}$. with $\lambda \mid p + 1$, be a curve as given in case (2.16) of Corollary 2.16. Then any standard form of C can be obtained by applying an isomorphism of the form in (2.5) through the procedure of Theorem 3.3 from the given model of C. In particular, the only standard form of C is $y^p - y = x^\lambda$.*

Proof The automorphisms of this curve are described in Lemma 2.19. When $\lambda \neq p + 1$, the order p subgroups are generated by

$$(x, y) \mapsto (x, y + 1) \ \text{ and } \ (x, y) \mapsto \left(\frac{x}{(y + 1)^{(p+1)/\lambda}}, \frac{y}{y + 1}\right).$$

They all produce curves of the form $y^p - y = x^\lambda$. When $\lambda = p + 1$, there are extra order p subgroups. Rewriting the equation as $y^p - y = x^{p+1}$, it suffices to consider the automorphisms $(x, y) \mapsto (x + a^p, y + ax + b)$ with $a^{p^2} + a = 0$ and $b^p - b - a^{p+1} = 0$, producing the degree p subextension $\overline{\mathbb{F}}_p(x^p + x, P)$ where P is the product of all the images of y under these automorphisms. This subextention is not isomorphic to $\overline{\mathbb{F}}_p(x)$, and hence neither to $\overline{\mathbb{F}}_p(\mathbb{P}^1)$. If it were, C would be birational to $x^p + x = 0$, but this curve is p copies of $\mathbb{P}^1$ and hence reducible. □

Remark 3.9 The upshot of Lemmas 3.6 and 3.8 is that there are only a finite number of standard forms for each isomorphism class of exceptional curves, and they can be easily enumerated. This confirms again that the group of isomorphisms between exceptional curves in standard form is finite.

4 Invariant Computations

In this section we determine invariants for curves within each stratum of $\mathcal{AS}_g$ for Artin-Schreier curves of genus $g = 3, 4$ in odd characteristic. As we see in Table 2, there is a single irreducible component in each stratum in these cases, so each stratum has a unique system of invariants.

4.1 Genus 3, Characteristic 3

In this case, the quantity D defined in (2.2) takes on the value $D = 3$. There are two partitions of $D + 2 = 5$ (up to reordering) that satisfy the conditions of Theorem 2.14, namely

$$\{5\} \quad \text{and} \quad \{3, 2\}, \tag{4.1}$$

so there are two strata in $\mathcal{AS}_g$. These partitions also determine the standard forms of all possible genus 3 Artin-Schreier curves in characteristic 3. Recall that $d_i = e_i - 1$ is the order of the pole P_{μ_i} of $f(x)$ for the Artin-Schreier curve $C_f : y^3 - y = f(x)$. The partitions in (4.1) show that C_f has either one pole of order 4 or two poles with respective orders 2 and 1. We treat these two cases separately below.

4.1.1 One Pole of Order 4

We use (2.4) in Theorem 2.14 with $D = 3$, $r = 0$, and $e_1 = 5$ to determine that the dimension of this stratum is

$$\dim \mathcal{AS}_{3,\{5\}} = 3 - 1 - \lfloor 4/3 \rfloor = 1.$$

We have $r = 0$ and $d_1 = 4 \equiv 1 \pmod 3$, corresponding to Case (1) of Theorem 3.3 and yielding a standard form

$$C : y^3 - y = x^4 + ax^2, \tag{4.2}$$

with $a \in \overline{\mathbb{F}}_3$. When $a = 0$, this curve is isomorphic to an exceptional curve of type (2.16) in Corollary 2.16 which has standard form $y^3 - y = x^4$. This is the only exceptional curve in the family, see Lemma 3.8.

Proposition 4.1 *Every isomorphism between curves in standard form as in* (4.2) *with* $a \neq 0$ *is given, up to composition with powers of* $\sigma : (x, y) \mapsto (x, y+1)$*, by*

$$(x, y) \mapsto (\alpha x, \lambda y), \tag{4.3}$$

where $\lambda \in \mathbb{F}_3^\times$ *and* $\alpha \in \overline{\mathbb{F}}_3$ *with* $\alpha^4 = \lambda$.

Proof Let C be as in Eq. (4.2). By Corollary 2.16, disregarding composition with powers of σ, every isomorphism φ of C is given by $\varphi_{\lambda,M}$ as in (3.2) with $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\overline{\mathbb{F}}_3)$. Since the image of C must be in standard form, $\varphi_{\lambda,M}$ must not move the pole at ∞, so $\gamma = 0$ and we can assume without loss of generality that $\delta = 1$. Since the coefficient of x in $\varphi_{\lambda,M}(C)$ must vanish, we conclude that $\beta = 0$, and that the unique polynomial $h(x)$ that produces a curve in standard form is $h(x) = 0$. So $\varphi_{\lambda,M}$ is of the form $(x, y) \mapsto (\alpha x, \lambda y)$. and yields the curve

$$\lambda(y^3 - y) = \alpha^4 x^4 + a\alpha^2 x^2.$$

Since the right-hand side must be monic in the standard form, we have $\alpha^4 = \lambda$. □

In the language of group actions, we now have a finite group $G \simeq \mathbb{Z}/4\mathbb{Z}$ acting on $\overline{\mathbb{F}}_3[a]$. This action is via isomorphisms of curve models of the form $y^3 - y = x^4 + ax^2$, sending $a \mapsto \epsilon a$ with $\epsilon^4 = 1$. We see that G acts linearly on $\overline{\mathbb{F}}_3[a]$.

Corollary 4.2 *The element* $I_1 = a^4$ *is an invariant and generates the ring of invariants for Artin-Schreier curves of genus* 3 *in characteristic* 3 *with* 3*-rank* 0*, i.e.,* $\overline{\mathbb{F}}_3[a]^G = \overline{\mathbb{F}}_3[I_1]$.

Proof It is straightforward to check that I_1 is an invariant for the action of G and forms a reconstructing set for the family (namely, different choices of a such that $a^4 = I_1$ for $y^3 - y = x^4 + ax^2$ produce isomorphic curves in standard form). By Corollary 2.13 we have $\overline{\mathbb{F}}_3[a]^G = \widetilde{\overline{\mathbb{F}}_3[I_1]} = \overline{\mathbb{F}}_3[I_1]$. □

Remark 4.3 This corollary can also be proved by computing a set of generators for $\overline{\mathbb{F}}_3[a]^G$ using Magma; or by manually checking for invariants up to degree 4 (see Lemma 2.8).

Remark 4.4 If we start with a model $y^3 - y = ax^4 + bx^3 + cx^2 + dx + e = p(x)$, the invariant I_1 (of a curve in the family $y^3 - y = x^4 + ax^2$ isomorphic to the starting curve) is given by c^4/a^2. More generally, if we start with $y^3 - y = \frac{ax^4+bx^3+cx^2+dx+e}{(x-\lambda)^4}$, the reconstructing invariant can be chosen to be $I_1 = c^4/(a\lambda^4 + b\lambda^3 + c\lambda^2 + d\lambda + e)^2$.

4.1.2 One Pole of Order 2 and One Pole of Order 1

We use (2.4) in Theorem 2.14 with $D = 3$, $r = 1$, $e_1 = 3$, and $e_2 = 2$ to determine that the dimension of this stratum is

$$\dim \mathcal{AS}_{3,\{3,2\}} = 3 - 1 - \lfloor 2/3 \rfloor - \lfloor 1/3 \rfloor = 2.$$

Based on Theorem 3.3, the standard form of curves with a pole of order 2 and a second pole of order 1 is

$$C\colon y^3 - y = x^2 + ax + \frac{b}{x} \tag{4.4}$$

for $a, b \in \overline{\mathbb{F}}_3$ with $b \neq 0$.

Proposition 4.5 *Every isomorphism between curves in standard form as in (4.4) is given, up to composition with powers of $\sigma : (x, y) \mapsto (x, y + 1)$, by*

$$(x, y) \mapsto (\alpha x, \lambda y), \tag{4.5}$$

where $\lambda \in \mathbb{F}_3^\times$ and $\alpha \in \overline{\mathbb{F}}_3$ with $\alpha^2 = \lambda$.

Proof No curve in this family is exceptional, so we can directly use Corollary 2.16 to see that, disregarding composition with powers of σ, every isomorphism is of the form $\varphi_{\lambda,M}$ as in (3.2) with $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\overline{\mathbb{F}}_3)$. In this particular case, each isomorphism must fix ∞ and 0, so $\gamma = \beta = 0$, and we can choose δ to be equal to 1. This implies that $h(x) = 0$, so the only isomorphisms of C as in (4.4) are of the form $(x, y) \mapsto (\alpha x, \lambda y)$. Applying the isomorphism to C and using the requirement that the right-hand side of a standard form must be monic yields $\alpha^2 = \lambda$, so there are four possible values for α since $\lambda \in \mathbb{F}_3^\times$. This produces the model

$$\widetilde{C}\colon y^3 - y = x^2 + a'x + \frac{b'}{x}, \tag{4.6}$$

where $a' = a/\alpha$ and $b' = b/\alpha^3$. Since a and b can take on any values in $\overline{\mathbb{F}}_3$, we obtain a two-dimensional family of curves from the isomorphism in (4.5). Since the stratum is two-dimensional, this isomorphism yields all curves with the prescribed poles and orders. □

These isomorphisms give a group action of the finite group $G \simeq \mathbb{Z}/4\mathbb{Z}$ acting linearly on $\overline{\mathbb{F}}_3[a, b]$. The action is generated by $(a, b) \mapsto (ia, -ib)$, where $i^2 = -1$.

Corollary 4.6 *The elements $I_1 = a^4$, $I_2 = ab$, and $I_3 = b^4$ generate the ring of invariants for Artin-Schreier curves of genus 3 in characteristic 3 with 3-rank 2, i.e., $\overline{\mathbb{F}}_3[a, b]^G = \overline{\mathbb{F}}_3[I_1, I_2, I_3]$. These elements satisfy the algebraic relation $I_1 I_3 - I_2^4 = 0$.*

Proof Let a' and b' denote the coefficients of $1/x$ and x in (4.6), respectively. Then $(a')^4 = (a/\alpha)^4 = a^4$ and $(b')^4 = (b/\alpha^3)^4 = b^4$ for all $\alpha \in \overline{\mathbb{F}}_3$. Hence I_1 and I_3 are invariants. Furthermore, $a'b' = ab/\alpha^4 = ab$, so I_2 is also an invariant. On the other hand, given values $\{I_1, I_2, I_3\}$ and choosing $a, b \in \overline{\mathbb{F}}_3$ with $a^4 = I_1$, $b^4 = I_3$ and $ab = I_2$, we can reconstruct a unique standard form model as in (4.4). Different choices of a and b yield isomorphic models. By Corollary 2.13 this implies that $\overline{\mathbb{F}}_3[a, b]^G = \overline{\mathbb{F}}_3[I_1, I_2, I_3]$. □

Remark 4.7 Given a more general model $y^3 - y = \frac{ax+b}{x-\lambda_1} + \frac{cx^2+dx+e}{(x-\lambda_2)^2}$, the set

$$\left\{\frac{(c\lambda_1\lambda_2 - d(\lambda_1+\lambda_2)+e)^4}{(c\lambda_2^2+d\lambda_2+e)^2}, \frac{(a\lambda_1+b)^4(c\lambda_2^2+d\lambda_2+e)^2}{(\lambda_1-\lambda_2)^8}, \frac{(c\lambda_1\lambda_2 - d(\lambda_1+\lambda_2)+e)(a\lambda_1+b)}{(\lambda_1-\lambda_2)^2}\right\}$$

is a reconstructing set of invariants.

4.2 Genus 3, Characteristic 7

There is only one component in this stratum since the only partition is {3}. In this case, there is only one pole of order 2 and a unique standard form:

$$y^7 - y = x^2.$$

Note that this is one of the exceptional curves in case (2) of Corollary 2.16.

4.3 Genus 4, Characteristic 3

This case has three strata, consisting of curves with respective 3-ranks 0, 2, and 4.

4.3.1 A Single Pole of Order 5

In this case the 3-rank is $s = 0$ by (2.3), and we have $\vec{E} = \{6\}$. This corresponds to a curve C_f where $f(x)$ has one pole of order 5. The standard form as given in Theorem 3.3 is:

$$C : y^3 - y = x^5 + cx^4 + dx^2 \tag{4.7}$$

for some $c, d \in \overline{\mathbb{F}}_3$. Note that none of the exceptional curves have a standard form of this type, so Corollary 2.16 applies to this stratum.

Identifying isomorphisms between standard forms in this case is cumbersome. However, it is fairly straightforward to compute invariants from a different model of the curve. We first apply isomorphisms to reach a different distinguished form, compute invariants using this model, and then express these invariants in terms of the coefficients in our standard form.

Lemma 4.8 *Every curve with standard form C given in (4.7) is isomorphic to one of the form*

$$C_g : y^3 - y = x^5 + ax^2 + bx \tag{4.8}$$

for some $a, b \in \overline{\mathbb{F}}_3$*. Specifically,* $a = c^3 + d$ *and* $b = (-cd - \epsilon^2)$*, where* $\epsilon^3 = c$*.*

Proof We apply the isomorphism $\varphi_{\lambda,M}$ from (3.2) to C, where $\lambda = 1$ and $M = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$, to obtain

$$y^3 - y = x^5 - c^2x^3 + (c^3 + d)x^2 - cdx + (-c^5 + c^2d) =: \tilde{f}(x).$$

Next, we determine a polynomial $h(x) = h_1x + h_2 \in \overline{\mathbb{F}}_3[x]$ such that $h(x)^3 - h(x)$ has the same x^3-term and constant term as $\tilde{f}$. Let $\epsilon \in \overline{\mathbb{F}}_3$ with $\epsilon^3 = c$. Comparing coefficients at x^3 yields $h_1^3 = -c^2$, so $h_1 = -\epsilon^2$. Comparing constant coefficients defines h_2 via the relation $h_2^3 - h_2 = -c^5 + c^2d$. Then C_f is isomorphic to

$$\begin{aligned} C_g : y^3 - y &= x^5 - c^2x^3 + (c^3 + d)x^2 - cdx + (-c^5 + c^2d) - \left((h_1x + h_2)^3 - (h_1x + h_2)\right) \\ &= x^5 + (c^3 + d)x^2 + (-cd - \epsilon^2)x. \end{aligned}$$

□

Proposition 4.9 *Every isomorphism between curves defined as in (4.8) is given, up to composition with powers of* $\sigma : (x, y) \mapsto (x, y + 1)$*, by*

$$(x, y) \mapsto (\alpha x, \alpha^5 y)$$

for some $\alpha \in \overline{\mathbb{F}}_3$ *with* $\alpha^{10} = 1$*.*

Proof Let $M := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\overline{\mathbb{F}}_3)$. Any isomorphism $\varphi_{\lambda,M}$ between curves of the form (4.8) must preserve the pole at infinity, implying $\gamma = 0$. Further, the requirement of a vanishing x^4 term forces $\beta = 0$, and thus $h(x) = 0$. The fact that the resulting form must be monic in x necessitates $\lambda^{-1}\alpha^5/\delta^5 = 1$. Without loss of generality, assume that $\delta = 1$, so $\lambda = \alpha^5$. Since $\lambda^2 = 1$, we must have $\alpha^{10} = 1$. □

These isomorphisms yield a group action of the finite group $G \simeq \mathbb{Z}/5\mathbb{Z}$ acting linearly on $\overline{\mathbb{F}}_3[a, b]$, generated by $(a, b) \mapsto (a/\alpha^3, b/\alpha^4)$ with $\alpha^{10} = 1$.

Corollary 4.10 *The elements* $I_1 = a^{10}$*,* $I_2 = b^5$*, and* $I_3 = a^2b$ *generate the ring of invariants for Artin-Schreier curves of genus* 4 *in characteristic* 3 *with* 3*-rank* 0*, i.e.,* $\overline{\mathbb{F}}_3[a, b]^G = \overline{\mathbb{F}}_3[I_1, I_2, I_3]$*. These elements satisfy the relation* $I_1I_2 = I_3^5$*.*

Proof For a curve C_g as in (4.8), we apply an isomorphism as given in Proposition 4.9 to obtain

$$C_{\tilde{g}} : y^3 - y = x^5 + \frac{a}{\alpha^3}x^2 + \frac{b}{\alpha^4}x.$$

It is easy to check that the given functions I_1, I_2, I_3. are invariant under this action. Conversely, given values $\{I_1, I_2, I_3\}$ with $I_1 I_2 = I_3^5$, we can choose $a, b \in \overline{\mathbb{F}}_3$ such that $a^{10} = I_1$, $b^5 = I_2$, in which case $a^2 b = I_3$. Suppose $I_1 = \tilde{a}^{10}$ and $I_2 = \tilde{b}^5$ with $\tilde{a}, \tilde{b} \in \overline{\mathbb{F}}_3$, and let $\alpha \in \overline{\mathbb{F}}_3$ be such that $\alpha^3 = \tilde{a}/a$. The relation $a^{10} = \tilde{a}^{10}$ implies that $\alpha^{10} = 1$, so $\alpha^4 = \tilde{a}^2/a^2$. Since $a^2 b = \tilde{a}^2 \tilde{b}$, we have $b/\alpha^4 = \tilde{b}$. Hence, the curves $y^3 - y = x^5 + ax^2 + bx$ and $y^3 - y = x^5 + \tilde{a}x^2 + \tilde{b}x$ are isomorphic via the isomorphism in Proposition 4.9 given by α with $\alpha^3 = \tilde{a}/a$. Corollary 2.13 now implies that I_1, I_2, and I_3 generate the invariant ring. □

By applying the change of variables from Lemma 4.8, we obtain the following.

Corollary 4.11 *Two curves in standard form as in (4.7) are isomorphic if and only if they have the same invariants* $I_1 = (c^3 + d)^{10}$, $I_2 = (-cd - \epsilon^2)^5$, *and* $I_3 = (c^3 + d)^2(-cd - \epsilon^2)$, *where* $\epsilon^3 = c$.

4.3.2 Two Poles of Order 2

This case corresponds to the partition $\vec{E} = \{3, 3\}$. According to Theorem 3.3, the curves in this stratum have standard form

$$C\colon y^3 - y = x^2 + ax + \frac{b}{x} + \frac{c}{x^2} \tag{4.9}$$

for $a, b, c \in \overline{\mathbb{F}}_3$ with $c \neq 0$.

Proposition 4.12 *Every isomorphism between curves in standard form as in (4.9) is given, up to composition with powers of* $\sigma : (x, y) \mapsto (x, y + 1)$, *by*

$$(x, y) \mapsto (\alpha x, \alpha^3 y), \tag{4.10}$$

where $\alpha^4 = 1$, *or by*

$$(x, y) \mapsto \left(\frac{1}{\gamma x}, \lambda y\right), \tag{4.11}$$

where $\lambda \in \mathbb{F}_3^\times$ *and* $c\gamma^2 = \lambda$.

Proof Let C be as in Eq. (4.9). Any isomorphism of C that yields another curve in standard form must either fix P_∞ and P_0 or swap these poles. We first consider the case when both poles are fixed. In this situation, once again disregarding composition by powers of σ, the isomorphism is of the form $\varphi_{\lambda, M_\alpha}$ for $M_\alpha = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$, with $\lambda \in \mathbb{F}_3^\times$ and $\alpha \in \overline{\mathbb{F}}_3^\times$. Applying $\varphi_{M_\alpha, \lambda}$ to C gives

$$y^3 - y = \frac{\alpha^2 x^2}{\lambda} + \frac{a\alpha x}{\lambda} + \frac{b}{\lambda \alpha x} + \frac{c}{\lambda \alpha^2 x^2}.$$

Since the image curve must be in standard form, we have $\alpha^2 = \lambda$, so $\alpha^4 = 1$. This isomorphism acts on the standard form model by $(a, b, c) \mapsto \left(\frac{1}{\alpha}a, \alpha b, c\right)$.

In the second case, when the poles are switched, the isomorphism must be of the form $\varphi_{\lambda, M_\gamma}$ for $M_\gamma = \begin{pmatrix} 0 & 1 \\ \gamma & 0 \end{pmatrix}$, with $\lambda \in \mathbb{F}_3^\times$ and $\gamma \in \overline{\mathbb{F}}_3^\times$. The image of C under $\varphi_{M_\gamma, \lambda}$ is

$$y^3 - y = \frac{c\gamma^2 x^2}{\lambda} + \frac{b\gamma x}{\lambda} + \frac{a}{\lambda \gamma x} + \frac{1}{\lambda \gamma^2 x^2}$$

so $c\gamma^2 = \lambda$. Since $\lambda^2 = 1$, the isomorphism acts on the coefficients of a curve in standard form given by Eq. (4.9) via $(a, b, c) \mapsto \left(\frac{\gamma b}{\lambda}, \frac{\lambda a}{\gamma}, c\right)$. □

The isomorphisms in Proposition 4.12 define a non-linear group action of the dihedral group $G \simeq D_4$ of order 8 on the function field $\overline{\mathbb{F}}_3(a, b, c)$. It cannot a priori be descended to the polynomial ring $\overline{\mathbb{F}}_3[a, b, c]$. We proceed as follows to obtain invariants in this case. With the notation in Eq. (4.11) in Proposition 4.12, we have $\left(\frac{\lambda}{\gamma}\right)^2 = \lambda c = \pm c$. This defines a linear action of the dihedral group D_4 of order 8 on the polynomial ring $\overline{\mathbb{F}}_3(\sqrt{c})[a, b]$ over the field $\overline{\mathbb{F}}_3(\sqrt{c})$. It is generated by $(a, b) \mapsto (ia, -ib)$ where $i^2 = -1$ and $(a, b) \mapsto \left(\frac{b}{\sqrt{c}}, \sqrt{c}a\right)$.

Lemma 4.13 *The elements $I_2 = ab$ and $I_3 = a^4c^2 - b^4$ generate $\overline{\mathbb{F}}_3(\sqrt{c})[a, b]^G$.*

Corollary 4.14 *Two curves in standard form as in Eqs. (4.9) are isomorphic if and only if they have the same invariants $I_1 = c$, $I_2 = ab$, and $I_3 = a^4c^2 - b^4$.*

4.3.3 Three Poles of Order 1

We now consider the stratum $\mathcal{AS}_{4,4}$ for $p = 3$. There is a single partition yielding $g = 4$ and $s = 4$, namely $\vec{E} = \{2, 2, 2\}$. From Table 2, we see that this component has dimension $\dim \mathcal{AS}_{4,\{2,2,2\}} = 3$. From Theorem 3.3, the standard form of a curve in this component is

$$C\colon y^3 - y = ax + \frac{b}{x} + \frac{c}{x - 1}, \tag{4.12}$$

where $a, b, c \in \overline{\mathbb{F}}_3^\times$.

Note that there is a subfamily of exceptional curves (see case (2.16) of Corollary 2.16) within this stratum, of the form $C_a = y^3 - y = \frac{a}{x^3 - x}$ for $a \in \overline{\mathbb{F}}_3^\times$. A standard form for this curve is given by $y^3 - y = -ax + \frac{a}{x} + \frac{a}{x-1}$.

Proposition 4.15 *Let C be as in (4.12). The curves in standard form that are isomorphic to C are the ones in Table 3.*

Proof Due to Corollary 2.16 and Lemma 3.6, isomorphisms, up to composition with powers of $\sigma : (x, y) \mapsto (x, y + 1)$, of these standard forms must be of the form

$$\varphi_{\lambda,M} : (x, y) \mapsto (Mx, \lambda y + h_M(x)),$$

where $\lambda \in \mathbb{F}_3^\times = \{\pm 1\}$ and $M \in \mathrm{GL}_2(\overline{\mathbb{F}}_3)$ permutes the poles P_∞, P_0, and P_1 in an S_3 action. This gives 6 choices of M and 2 choices of λ, yielding at most 12 labeled models. These 12 models are all distinct, and the action of the isomorphisms on C is described in Table 3. We compute a sample entry to demonstrate the process. To

Table 3 Action of the isomorphism $\varphi_{\lambda,M}$ on the coefficients of (4.12)

λ	Permutation	Matrix M	$f(x)$
1	(P_∞)	$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$	$ax + \frac{b}{x} + \frac{c}{x-1}$
1	$(P_\infty P_0)$	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$	$bx + \frac{a}{x} - \frac{c}{x-1}$
1	$(P_\infty P_1 P_0)$	$\begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix}$	$-bx + \frac{c}{x} - \frac{a}{x-1}$
1	$(P_\infty P_0 P_1)$	$\begin{pmatrix}-1 & 1\\ -1 & 0\end{pmatrix}$	$-cx - \frac{a}{x} + \frac{b}{x-1}$
1	$(P_0 P_1)$	$\begin{pmatrix}1 & -1\\ 0 & -1\end{pmatrix}$	$-ax - \frac{c}{x} - \frac{b}{x-1}$
1	$(P_\infty P_1)$	$\begin{pmatrix}-1 & 0\\ -1 & 1\end{pmatrix}$	$cx - \frac{b}{x} + \frac{a}{x-1}$
-1	(P_∞)	$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$	$-ax - \frac{b}{x} - \frac{c}{x-1}$
-1	$(P_\infty P_0)$	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$	$-bx - \frac{a}{x} + \frac{c}{x-1}$
-1	$(P_\infty P_1 P_0)$	$\begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix}$	$bx - \frac{c}{x} + \frac{a}{x-1}$
-1	$(P_\infty P_0 P_1)$	$\begin{pmatrix}-1 & 1\\ -1 & 0\end{pmatrix}$	$cx + \frac{a}{x} - \frac{b}{x-1}$
-1	$(P_0 P_1)$	$\begin{pmatrix}1 & -1\\ 0 & -1\end{pmatrix}$	$ax + \frac{c}{x} + \frac{b}{x-1}$
-1	$(P_\infty P_1)$	$\begin{pmatrix}-1 & 0\\ -1 & 1\end{pmatrix}$	$-cx + \frac{b}{x} - \frac{a}{x-1}$

exchange P_∞ and P_0 while fixing P_1, we solve using the reasoning in Sect. 3.1 to find $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. The effect of M on $f(x) = ax + \frac{b}{x} + \frac{c}{x-1}$ is

$$\begin{aligned} M(f(x)) &= \frac{a}{x} + bx + \frac{c}{\frac{1}{x} - 1} \\ &= bx + \frac{a}{x} + \frac{-c}{x-1} - c. \end{aligned}$$

We convert the corresponding curve equation to standard form, which is accomplished by sending $y \mapsto y + m$, where $m \in \overline{\mathbb{F}}_3$ such that $m^3 - m = -c$. This yields the standard form

$$\varphi_{\lambda,M}(C) : y^3 - y = bx + \frac{a}{x} + \frac{-c}{x-1}.$$ □

These isomorphisms define a linear action of a group $G \simeq D_6$, the dihedral group of 12 elements, generated by $(a, b, c) \mapsto (c, a, -b)$ and $(a, b, c) \mapsto (b, a, -c)$ on the polynomial ring $\overline{\mathbb{F}}_3[a, b, c]$.

Corollary 4.16 *The elements $I_1 = (abc)^2$, $I_2 = (abc)(a - b - c)$, $I_3 = ab + ac - bc$, and $I_4 = a^2 + b^2 + c^2$ generate the ring of invariants for Artin-Schreier curves of genus 4 in characteristic 3 with 3-rank 4, i.e., $\overline{\mathbb{F}}_3[a, b, c]^G = \overline{\mathbb{F}}_3[I_1, I_2, I_3, I_4]$. These elements satisfy the relation $I_1(I_3 + I_4) = I_2^2$.*

Proof A model as in (4.12) can be reconstructed from this set of invariants through a naive solve-and-back-substitution procedure that results in a polynomial equation of degree 6. Since all the roots of this equation belong to an (at most degree 6) extension of the (finite) field of definition of the invariants, there is a solution that defines coefficients for (4.12). □

Remark 4.17 The exceptional curves in this family occur exactly when $I_2 = I_3 = I_4 = 0$.

4.4 Genus 4, Characteristic 5

In this case there are two strata.

4.4.1 One Pole of Order 3

Here, the 5-rank is $s = 0$ and we have $\vec{E} = \{4\}$. This corresponds to a curve C_f where f has one pole of order 3, with standard form as given in case (1) of Theorem 3.3:

$$C : y^5 - y = x^3 + ax^2 \tag{4.13}$$

with $a \in \overline{\mathbb{F}}_5$. When $a = 0$, the curve has additional automorphisms as in Lemma 2.19.

Proposition 4.18 *Every isomorphism between curves in standard form as in* (4.13) *is given, up to composition with powers of* $\sigma : (x, y) \mapsto (x, y+1)$, *by* $\varphi_{\lambda,M}$ *with* $\lambda = \alpha^3$ *and* $M = \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}$, *where* $\alpha \in \overline{\mathbb{F}}_5$ *with* $\alpha^{12} = 1$ *and* $\beta \in \{0, -\frac{2a}{3}\}$.

Proof Let $M := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\overline{\mathbb{F}}_5)$. Any isomorphism $\varphi_{\lambda,M}$ between standard forms given by (4.13) must preserve the pole at infinity, so $\gamma = 0$. Without loss of generality, assume $\delta = 1$. We then obtain the image curve with model

$$y^5 - y = \frac{1}{\lambda}\alpha^3 x^3 + (3\alpha^2\beta + a\alpha^2)x^2 + (3\alpha\beta^2 + 2a\alpha\beta)x + a\beta^2.$$

Since the right-hand side must be monic, we have $\alpha^3 = \lambda$. Since $\lambda \in \mathbb{F}_5^\times$, $\lambda^4 = 1$, so $\alpha^{12} = 1$. Furthermore, since the standard form requires a vanishing x-term, it follows that $3\alpha\beta^2 + 2a\alpha\beta = 0$, so $\beta = -\frac{2a}{3}$ or $\beta = 0$. Finally, we choose an appropriate $h(x) = h_0 \in \overline{\mathbb{F}}_5$ to eliminate the constant term $a\beta^2$. $\square$

We obtain a linear action of a group $G \simeq \mathbb{Z}/12\mathbb{Z}$ generated by $a \mapsto \alpha a$ with $\alpha^{12} = 1$ on the polynomial ring $\overline{\mathbb{F}}_5[a]$.

Corollary 4.19 *The element* $I_1 = a^{12}$ *generates the ring of invariants for Artin-Schreier curves of genus* 4 *in characteristic* 5 *with* 5*-rank* 0, *i.e.,* $\overline{\mathbb{F}}_5[a]^G = \overline{\mathbb{F}}_5[I_1]$.

Proof It is straightforward to check that $\{I_1\}$ is invariant and a reconstructing set. Now apply Corollary 2.13. $\square$

4.4.2 Two Poles of Order 1

In this case the 5-rank is $s = 4$ and we have $\vec{E} = \{2, 2\}$. This corresponds to a curve C_f where f has two poles of order 1, with standard form as given in case (2) of Theorem 3.3:

$$y^5 - y = x + \frac{a}{x} \tag{4.14}$$

with $a \in \overline{\mathbb{F}}_5^\times$.

Proposition 4.20 *Every isomorphism between curves in standard form as in* (4.14) *is given, up to composition with powers of* $\sigma : (x, y) \mapsto (x, y+1)$, *by*

$$(x, y) \mapsto (\lambda x, \lambda y) \tag{4.15}$$

or by

$$(x, y) \mapsto \left(\frac{a}{\lambda x}, \lambda y\right), \tag{4.16}$$

where $\lambda \in \mathbb{F}_5^\times$.

Proof Let $M := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\overline{\mathbb{F}}_5)$ and $\lambda \in \mathbb{F}_5^\times$. Any isomorphism $\varphi_{\lambda,M}$ between standard forms here must either fix the poles P_∞ and P_0 or swap them. So, up to scalar multiple, M must be of the form $M_\alpha = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$ or $M_\gamma = \begin{pmatrix} 0 & 1 \\ \gamma & 0 \end{pmatrix}$. Let $f(x) = x + \frac{a}{x}$. In the first case, we obtain

$$\varphi_{\lambda,M_\alpha}(C_f) : y^5 - y = \frac{\alpha}{\lambda}x + \frac{a}{\alpha\lambda x}.$$

Since the polynomial part on the right-hand side must be monic, we must have $\alpha = \lambda$, leading to the standard form $y^5 - y = x + \frac{a}{\lambda^2 x}$ for $\varphi_{\lambda,M_\alpha}(C_f)$. So the isomorphism acts on the standard form model by sending $a \mapsto \frac{a}{\lambda^2} = \lambda^2 a$. In the second case, the image curve is

$$\varphi_{\lambda,M_\gamma}(C_f) : y^5 - y = \frac{1}{\lambda\gamma x} + \frac{a\gamma x}{\lambda}.$$

Again, since the polynomial part must be monic in standard form, we have $a\gamma = \lambda$, so the standard form of $\varphi_{\lambda,M_\gamma}(C_f)$ can be simplified to $y^5 - y = x + \frac{a}{\lambda^2 x}$. This isomorphism again acts on the standard form model by sending $a \mapsto \frac{a}{\lambda^2} = \lambda^2 a$. $\square$

We obtain a linear action of a group $G \simeq \mathbb{Z}/2\mathbb{Z}$ generated by $a \mapsto -a$ on the polynomial ring $\overline{\mathbb{F}}_5[a]$.

Corollary 4.21 *The element $I_1 = a^2$ generates the ring of invariants for Artin-Schreier curves of genus* 4 *in characteristic* 5 *with* 5*-rank* 4*, i.e.,* $\overline{\mathbb{F}}_5[a]^G = \overline{\mathbb{F}}_5[I_1]$.

Proof The set $\{I_1 = a^2\}$ is a reconstructing set for curves in the stratum with standard form as in (4.14). $\square$

Remark 4.22 The curves in this family are all hyperelliptic, but of characteristic different from 2. They can be written as $v^2 = u^{10} - 2u^6 + u^2 - 4a$ with $v = 2x - y^5 + y$ and $u = y$. Invariants for them inside the family of hyperelliptic curves of genus 4 in characteristic 5 (so inside a larger family) could also be computed with the techniques of [LR12].

5 Conclusion

In this paper, we determined reconstructing invariants for Artin-Schreier curves of genus 3 and 4 in characteristic $p > 2$. Our results on genus 3 represent an important step toward the full characterization of invariants of curves of that genus.

Moving to higher genus curves presents many additional challenges. In particular, curves C_f where f has many poles of the same order exhibit many ismorphisms between standard forms. As the genus grows, the problem becomes more and more complicated. Instead of seeking a general closed form for invariants of all Artin-Schreier curves, an algorithmic method of determining invariants seems appropriate.

Devising the right framework and specializing the results of invariant theory to this setting is the subject of ongoing work.

Acknowledgements The authors thank the Banff International Research Station for Mathematical Innovation and Discovery in Banff (Canada) for sponsoring the Women in Numbers 6 (WIN6) workshop and for providing a productive and enjoyable environment for our initial work on this project. We would especially like to thank the organizers of WIN6, Shabnam Akhtari, Alina Bucur, Jennifer Park, and Renate Scheidler, for making the conference and this collaboration possible. We are indebted to Rachel Pries for helpful conversations around this work. Last but not least, we wish to thank the anonymous referee for useful comments and suggestions. The research of the first author is partially supported by the Simons Foundation grant #550023. The research of the second author is in part supported by National Science Foundation Grant DMS-2201085 and by the School of Natural and Behavioral Sciences at Brooklyn College, City University of New York. The research of the third author is partially funded by the Melodia ANR-20-CE40-0013 project and the 2023-08 Germaine de Staël project. The research of the fourth author is supported by the National Science Foundation under grant DMS-2137661. Lastly, the research of the fifth author is funded by the Natural Sciences and Engineering Research Council of Canada (NSERC) (funding RGPIN-2019-04844).

References

[AS27] Emil Artin and Otto Schreier. Eine Kennzeichnung der reell abgeschlossenen Körper. In *Abh. Math. Sem. Hamburg*, volume 5, pages 225–231. Springer, 1927.

[Bas15] Romain Basson. *Arithmétique des espaces de modules des courbes hyperelliptiques de genre 3 en caractéristique positive*. PhD thesis, Université de Rennes 1, Rennes, 2015.

[BCK21] Irene Bouw, Nirvana Coppola, Pınar Kılıçer, Sabrina Kunzweiler, Elisa Lorenzo García, and Anna Somoza. Reduction types of genus-3 curves in a special stratum of their moduli space. In *Women in Numbers Europe III—Research Directions in Number Theory*, volume 24 of *Assoc. Women Math. Ser.*, pages 115–162. Springer, Cham, 2021.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BDF12] Alina Bucur, Chantal David, Brooke Feigon, Matilde Lalın, and Kaneenika Sinha. Distribution of zeta zeroes of Artin–Schreier covers. *Math. Res. Lett*, 19(06):1329–1356, 2012.

[BDFL16] Alina Bucur, Chantal David, Brooke Feigon, and Matilde Lalin. Statistics for ordinary Artin–Schreier covers and other p-rank strata. *Trans. AMS*, 368(4):2371–2413, 2016.

[BHM16] Irene Bouw, Wei Ho, Beth Malmskog, Renate Scheidler, Padmavathi Srinivasan, and Christelle Vincent. Zeta functions of a class of Artin-Schreier curves with many automorphisms. In *Directions in Number Theory*, volume 3 of *Assoc. Women Math. Ser.*, pages 87–124. Springer, [Cham], 2016.

[CFA06] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[Dix87] Jacques Dixmier. On the projective invariants of quartic plane curves. *Adv. in Math.*, 64(3):279–304, 1987.

[DK02] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

[DK08] Harm Derksen and Gregor Kemper. Computing invariants of algebraic groups in arbitrary characteristic. *Adv. Math.*, 217(5):2089–2129, 2008.

[Dol03] Igor Dolgachev. *Lectures on invariant theory*, volume 296 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2003.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[Eis05] David Eisenbud. *The geometry of syzygies*, volume 229 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005. A second course in commutative algebra and algebraic geometry.

[Ent12] Alexei Entin. On the distribution of zeroes of Artin–Schreier L-functions. *Geom. Funct. Anal.*, 22(5):1322–1360, 2012.

[Far10] Shawn Farnell. *Artin-Schreier curves*. PhD thesis, Colorado State University, Fort Collins, Colorado, 2010.

[Hen78] Hans-Wolfgang Henn. Funktionenkörper mit grosser Automorphismengruppe. *J. Reine Angew. Math.*, 302:96–115, 1978.

[HKT08] 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.

[Igu60] Jun-ichi Igusa. Arithmetic variety of moduli for genus two. *Ann. of Math. (2)*, 72:612–649, 1960.

[KLS20] Pınar Kılıçer, Elisa Lorenzo García, and Marco Streng. Primes dividing invariants of CM Picard curves. *Canad. J. Math.*, 72(2):480–504, 2020.

[Kon09] Aristides Kontogeorgis. Field of moduli versus field of definition for cyclic covers of the projective line. *J. Théor. Nombres Bordeaux*, 21(3):679–692, 2009.

[Liu93] Qing Liu. Courbes stables de genre 2 et leur schéma de modules. *Math. Ann.*, 295(2):201–222, 1993.

[Liu02] Qing Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford University Press, 2002.

[LLLR21] Reynald Lercier, Qing Liu, Elisa Lorenzo García, and Christophe Ritzenthaler. Reduction type of smooth plane quartics. *Algebra Number Theory*, 15(6):1429–1468, 2021.

[LR12] Reynald Lercier and Christophe Ritzenthaler. Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects. *J. Algebra*, 372:595–636, 2012.

[Mum65] David Mumford. *Geometric invariant theory*. Ergebnisse der Mathematik und ihrer Grenzgebiete, (N.F.), Band 34. Springer-Verlag, Berlin-New York, 1965.

[Noe26] E. Noether. Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p. *Nachrichten von der Gesellschaft der Wissenschaften zu Gŏttingen, Mathematisch-Physikalische Klasse*, 1926:28–35, 1926.

[Ohn07] Toshiaki Ohno. The graded ring of invariants of ternary quartics I, 2007. unpublished.

[PZ12] Rachel Pries and Hui June Zhu. The p-rank stratification of Artin-Schreier curves. *Ann. Inst. Fourier (Grenoble)*, 62(2):707–726, 2012.

[Shi67] Tetsuji Shioda. On the graded ring of invariants of binary octavics. *Amer. J. Math.*, 89:1022–1046, 1967.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer Science & Business Media, 2009.

[Sub75] Doré Subrao. The p-rank of Artin–Schreier curves. *Manuscripta Math.*, 16(2):169–193, 1975.

[Sym11] Peter Symonds. On the Castelnuovo-Mumford regularity of rings of polynomial invariants. *Ann. of Math. (2)*, 174(1):499–517, 2011.

[vdGvdV91] Gerard van der Geer and Marcel van der Vlugt. Artin-Schreier curves and codes. *J. Algebra*, 139(1):256–272, 1991.

[vdGvdV92] Gerard van der Geer and Marcel van der Vlugt. Reed-Muller codes and supersingular curves. I. *Compos. Math.*, 84(3):333–367, 1992.

[VM80] Robert C. Valentini and Manohar L. Madan. A hauptsatz of L. E. Dickson and Artin-Schreier extensions. *J. Reine Angew. Math.*, 318:156–177, 1980.