DISSERTATION

ARTIN-SCHREIER CURVES

Submitted by

Shawn Farnell

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Fall 2010

COLORADO STATE UNIVERSITY

July 28, 2010

WE HEREBY RECOMMEND THAT THE DISSERTATION PREPARED UNDER OUR SUPERVISION BY SHAWN FARNELL ENTITLED ARTIN-SCHREIER CURVES BE ACCEPTED AS FULFILLING IN PART REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY.

Committee on Graduate Work

Jeff Achter

Chris Peterson

Martin Gelfand

Advisor: Rachel Pries

Department Head: Simon Tavener

ABSTRACT OF DISSERTATION

ARTIN-SCHREIER CURVES

Let k be an algebraically closed field of characteristic p where p is a prime number. The main focus of this work is on properties of Artin-Schreier curves. In particular, we study two invariants of the p-torsion of the Jacobian of these curves: the p-rank and the a-number. In the main result, we demonstrate a family of Artin-Schreier curves for which the a-number is constant. We also give a result concerning the existence of deformations of Artin-Schreier curves with varying p-rank.

Shawn Farnell
Department of Mathematics
Colorado State University
Fort Collins, Colorado 80523
Fall 2010

ACKNOWLEDGMENTS

There are many people that I would like to thank for making my time in graduate school wonderful. First, I would like to say thank you to the faculty and staff of the math department. You make this an enjoyable place to work and learn. Second, I would like to thank the graduate students of the math department. Your willingness to work together, study late into the night, and socialize with each other make this department special. Third, I would like to say thank you to my committee members: Jeff Achter, Chris Peterson, Martin Gelfand, and Ross McConnell. Thank you for sharing your advice, comments, and motivation at each step of the way. Fourth, I would like to thank the students of Colorado State University. My passion for teaching developed in the classrooms you filled. And most of all, I would like to thank my advisor Dr. Rachel Pries for sharing five years of her time and energy with me. Her guidance, expertise, and patience have put me where I am today.

I would also like to thank my family and friends for their love and support. And last of all, thank you to my brothers for the academic peer pressure.

Contents

Chapter 1

Introduction

The main focus of this thesis is on properties of Artin-Schreier curves. Let k be an algebraically closed field of characteristic p where $p > 0$ is prime. Then, an Artin-Schreier curve is a smooth projective k-curve X given by an affine equation $y^p - y = f(x)$ for some $f(x) \in k(x)$. In order for this curve to be connected, we require that $f(x) \neq z^p - z$ for any $z \in k(x)$. Artin-Schreier curves are cyclic degree p covers of the projective k-line.

Artin-Schreier curves often yield examples of interesting phenomena. For this reason, Artin-Schreier curves have been studied a lot in recent years. For instance, the Newton polygons of Artin-Schreier curves have been studied in [1, 2, 3, 13, 16]. In [6, 21, 22], the focus is on Artin-Schreier curves with many rational points defined over finite fields. This is also the case in [20] where the focus is on coding theory using Artin-Schreier curves. The zeta functions of Artin-Schreier curves over finite fields are considered in [10, 11]. While this list is far from complete, it is clear the Artin-Schreier curves are an active area of research.

To each curve X, there is an associated abelian variety called the Jacobian, Jac(X). To study the Jacobian of X, we look at the multiplication-by-p morphism. The kernel of this map is denoted by Jac$(X)[p]$ and is called the p-torsion of the Jacobian of X. Because the multiplication-by-p morphism is inseparable, Jac$(X)[p]$

has the structure of a group scheme. Two invariants of the p-torsion of the Jacobian of a curve X are the p-rank and the a-number. To define these invariants, let μ_p and α_p denote the group schemes which are the kernel of Frobenius on $\mathbb{G}_m$ and $\mathbb{G}_a$, respectively. As schemes, $\mu_p = \text{Spec}\,(k[x]/(x^p-1))$ and $\alpha_p = \text{Spec}\,(k[x]/(x^p))$. The p-rank of X is $s_X = \dim_{\mathbb{F}_p}\text{Hom}\,(\mu_p, \text{Jac}(X)[p])$. The number s_X is the integer which satisfies $\#\text{Jac}(X)[p](k) = p^{s_X}$. The a-number of X is $a_X = \dim_k\text{Hom}\,(\alpha_p, \text{Jac}(X)[p])$. If g is the genus of X, the p-rank and a-number satisfy the inequalities $0 \leq s_X \leq g$ and $1 \leq s_X + a_X \leq g$.

The a-number of a curve X can be computed via the Cartier operator on the sheaf of holomorphic 1-forms of X. The modified Cartier operator is a $1/p$-linear map $\mathcal{C} : H^0(X, \Omega^1_X) \to H^0(X, \Omega^1_X)$ taking exact differentials to zero and satisfying $\mathcal{C}(f^{p-1}df) = df$. If β is a basis for $H^0(X, \Omega^1_X)$, let $\tilde{M}$ be the matrix which gives the action of the modified Cartier operator on β. The matrix M formed by taking each entry of $\tilde{M}$ to the p^{th} power is called the Cartier-Manin matrix and it gives the action of the Cartier operator. The a-number of X is then $a_X = g - \text{rank}(M)$, where g is the genus of X.

For the main result of the paper, we consider an Artin-Schreier curve $X : y^p - y = f(x)$ where $f(x) \in k(x)$. Let $r+1$ be the number of poles of $f(x)$. For $1 \leq j \leq r+1$, let d_j be the order of the j^{th} pole of $f(x)$. We assume that each d_j divides the quantity $p-1$. In this case, the Riemann-Hurwitz formula [18] gives that the genus of X is $g = \left(\sum_{i=1}^{r+1}(d_j+1) - 2\right)\cdot(p-1)/2$ and the Deuring-Shafarevich formula [9] gives that the p-rank of X is $s_X = r(p-1)$. With this setup, we prove the following theorem in chapter 3.

Theorem 1. *Let X be an Artin-Schreier curve with affine equation $y^p - y = f(x)$, with $f(x) \in k(x)$. Suppose $f(x)$ has $r+1$ poles, with orders $\{d_1, \ldots, d_{r+1}\}$. If each d_j divides $p-1$, the a-number of X is*

$$a_X = \sum_{j=1}^{r+1} a_j, \text{ where}$$

$$a_j = \begin{cases} \frac{(p-1)d_j}{4} & \text{if } d_j \text{ even} \\ \frac{(p-1)(d_j-1)(d_j+1)}{4d_j} & \text{if } d_j \text{ odd.} \end{cases}$$

In particular, the a-number of X only depends on the orders of the poles of $f(x)$ and otherwise does not depend on the equation for X. This is the first example known of a family of curves for which the a-number is constant and greater than three. Theorem 1 shows that the a-number of each curve in this family is roughly half of the genus. Using [15, Theorem 1.1 (2)], the dimension of this family can be computed to be $\sum_{i=1}^{r+1}(d_j+1) - 3 = 2g/(p-1) - 1$.

This result can be situated in the context of other results about Artin-Schreier curves and the p-rank and a-numbers of curves [4, 5, 7, 14]. Specifically, it generalizes [14, Corollary 3.3 (1)]. A few of these results are described in section 2.7.

In Section 4.6.1, a deformation result is given for Artin-Schreier curves. Specifically, we give a scenario under which it is possible for an Artin-Schreier cover with one branch point to deform to an Artin-Schreier cover with three branch points. This increases the p-rank by $2(p-1)$. This result builds on previous deformation results [12, 15].

Theorem 2. *Let X be an Artin-Schreier curve of genus $g = (p-1)(d-1)/2$ and p-rank 0. It is given by an affine equation $y^p - y = f(x)$ for some degree d polynomial $f(x) \in k[x]$ with $d \not\equiv 0 \bmod p$. Assume $d \geq 2p+1$ and $f(x) \in x^d k\left[x^{-p}\right]$. Then, there exists a flat deformation of X over Spec$(k[[t]])$ whose generic fibre is an Artin-Schreier curve with p-rank $2(p-1)$.*

This result gives some information about the geometry of the moduli space of Artin-Schreier curves. This deformation is realized by an equation of the form

$$y^p - y = \frac{f(x)}{(1-xt)^b(1+xt)^c},$$

where b and c satisfy certain numerical conditions.

The paper begins with background information on Artin-Schreier curves. It is here that we discuss the genus, the p-rank, and the a-number of an Artin-Schreier curve. In Chapter 3, we state and prove Theorem 1. Chapter 4 will focus on the moduli space of Artin-Schreier curves. In Section 4.6, we state and prove Theorem 2.

The main result of this paper, which appears in Chapter 3, was discovered through a computer program written in the computer algebra system Maple. This code appears in Appendix C. Also in the Appendix are sections about the Riemann-Hurwitz formula (Appendix A) and supersingular elliptic curves (Appendix B).

Chapter 2

Artin-Schreier curves

Let k be an algebraically closed field of characteristic $p > 0$. An Artin-Schreier curve is a smooth projective connected k-curve Y with affine equation $y^p - y = f(x)$ where $f(x) \in k(x)$. We first notice that if $(x, y) \in \mathbb{A}^2_k$ is in the variety $Y_0 = V(y^p - y - f(x))$ then so is the point $(x, y + 1)$.

$$\begin{aligned}(y+1)^p - (y+1) &= (y^p + 1) - (y+1) \\ &= y^p - y \\ &= f(x).\end{aligned}$$

Let $B \subset \mathbb{P}^1(k)$ be the set of poles of $f(x)$. The cover $Y_0 \to \mathbb{P}^1_k - B$ corresponds to the field extension

$$k(x) \to \frac{k(x)[y]}{(y^p - y - f(x))}.$$

From the work above, we can see that one element of the Galois group is given by $\sigma : x \mapsto x, y \mapsto y + 1$. Since the field extension has degree p and σ has order p, we see the Galois group is cyclic of order p. Thus an Artin-Schreier curve is a cover ϕ of the projective line with Galois group $\mathbb{Z}/p$.

2.1 Standard form

First, we look at the special case when the Artin-Schreier curve is defined by a polynomial.

Proposition 2.1.1. *Given an Artin-Schreier curve of the form $y^p - y - f(x)$ where $f(x) \in k[x]$ has degree n, there is an isomorphism with an Artin-Schreier curve $y^p - y - g(x)$, where $g(x)$ is a polynomial with the following form:*

1. *$g(x)$ is a monic polynomial of degree $d \leq n$ where $p \nmid d$, and $d = n$ if $p \nmid n$,*
2. *the coefficient of x^{d-1} is zero,*
3. *the coefficient of x^m is zero for $m \equiv 0$ mod p.*

Proof. This is done through changes of variables as follows. Suppose we are given an Artin-Schreier curve $y^p - y = f(x)$ where $f(x) = a_n x^n + \ldots + a_0$, $a_n \neq 0$. Assume that n is not divisible by p. If n is divisible by p we can use a change of variables similar to the one we will use to show property three. We can achieve the first property above by letting $x = x_1 \cdot (a_n)^{-1/n}$ and substituting this into the equation for our curve. Our original curve is then isomorphic to the curve given by $y^p - y = f_1(x_1)$ where

$$\begin{aligned} f_1(x_1) &= f(x) \\ &= f(x_1 \cdot (a_n)^{-1/n}) \\ &= a_n(x_1 \cdot (a_n)^{-1/n})^n + a_{n-1}(x_1 \cdot (a_n)^{-1/n})^{n-1} + \ldots + a_0 \\ &= x_1^n + b_{n-1}x^{n-1} + \ldots + b_0 \end{aligned}$$

and $b_i = a_i \cdot ((a_n)^{-1/n})^i$ for $i \in \{0, \ldots, n-1\}$. Notice that f_1 is a monic polynomial.

To achieve the second property above, we let $x_1 = x_2 - \frac{1}{n}b_{n-1}$. Substituting this

into $f_1(x_1)$, we get

$$\begin{aligned} f_2(x_2) &= f_1(x_2 - \frac{1}{n}b_{n-1}) \\ &= (x_2 - \frac{1}{n}b_{n-1})^n + b_{n-1}(x_2 - \frac{1}{n}b_{n-1})^{n-1} + \ldots + b_0 \\ &= x_2^n - b_{n-1}x_2^{n-1} + \cdots + b_{n-1}x_2^{n-1} + \ldots + b_0 \\ &= x_2^n + c_{n-2}x_2^{n-2} + \ldots + c_0. \end{aligned}$$

In the second to last step, we showed that the two terms with an exponent of $n-1$ cancel. We leave out the calculation of the coefficients c_i in the last step. We now have that our original curve is isomorphic to $y^p - y = f_2(x_2)$ where f_2 is a degree n monic polynomial with no term of degree $n-1$.

For the third property, we can use a change of variables to get rid of the terms of f_2 which have an exponent divisible by p. Suppose $m = c \cdot p, c \neq 0$ and that we have a term $c_m x_2^m$ in f_2. Since k is algebraically closed, $c_m^{1/p} \in k$. Let $y = y_1 + (c_m)^{1/p} \cdot (x_2)^c$. Substituting this into the left side of the equation $y^p - y = f_2(x_2)$ we get

$$\begin{aligned} y^p - y &= \left(y_1 + (c_m)^{1/p} \cdot (x_2)^c\right)^p - \left(y_1 + (c_m)^{1/p} \cdot (x_2)^c\right) \\ &= y_1^p + c_m x_2^{c \cdot p} - y_1 - (c_m)^{1/p} \cdot (x_2)^c \\ &= y_1^p - y_1 + c_m x_2^m - (c_m)^{1/p} \cdot (x_2)^c. \end{aligned}$$

From this, we can see that the $c_m x_2^m$ term is on both sides of the equation and will cancel out. We also see that we get a new term $-(c_m)^{1/p} \cdot (x_2)^c$. Since c is smaller than m, we see that we can use this change of variables to get rid of all terms which have an exponent $m = c \cdot p$ by starting with the biggest such m and working down. We have now shown that our original curve $y^p - y = f(x)$ is isomorphic to the curve defined by $y_1^p - y_1 = h(x_2)$ where $h(x_2)$ has properties one, two, and leaving out the case when $m = 0$, property three above. So we only need to consider the case $m = 0$. For this, let $y_1 = y_2 + r$. Substituting this into the left side of $y_1^p - y_1 = h_2(x_2)$

gives

$$\begin{aligned} y_1^p - y_1 &= (y_2 + r)^p - (y_2 + r) \\ &= y_2^p - y_2 + r^p - r. \end{aligned}$$

Since k is algebraically closed, we can choose $r \in k$ so that $r^p - r$ is equal to the constant term of h_2. Then we get exactly the properties listed above. □

If an Artin-Schreier curve is given by $y^p - y - f(x)$ where $f \in k(x)$, we can still put it in a standard form. We can use similar changes of variables as above and a partial fraction decomposition to find an isomorphism between this curve and the curve

$$y^p - y = g_\infty(x) + \sum_{i=1}^{r} \frac{g_i(x - \alpha_i)}{(x - \alpha_i)^{d_i}}.$$

In this standard form, g_∞ has no terms with an exponent divisible by p. Also, each

$$\begin{aligned} \frac{g_i(x - \alpha_i)}{(x - \alpha_i)^{d_i}} &= \frac{c_0 + c_1(x - \alpha_i) + \ldots + c_t(x - \alpha_i)^{d_i - 1}}{(x - \alpha_i)^{d_i}} \\ &= \sum_{j=0}^{d_i - 1} c_j (x - \alpha_i)^{j - d_i} \end{aligned}$$

can be written so that the exponents $j - d_i$ are not divisible by p.

2.2 Genus of an Artin-Schreier curve

The genus of a curve X is the dimension of the vector space of holomorphic 1-forms on X over k. Let the regular differential 1-forms of $X : y^p - y = f(x)$ be denoted $H^0(X, \Omega_X^1)$. Then the genus of X is

$$g = \dim_k \left(H^0(X, \Omega_X^1) \right).$$

We assume that the Artin-Schreier curve is given by $y^p - y = f(x)$ where $f(x) \in k(x)$ is a rational function.

Proposition 2.2.1. *Suppose $y^p - y = f(x)$, where $f(x) \in k(x)$, defines an Artin-Schreier extension $\phi : Y \to \mathbb{P}^1(k)$. If $f(x)$ has a pole of order d, $p \nmid d$, at a point P, then the ramification index of ϕ at the point P' above P is $e(P'|P) = p$ and the degree of the different at P' is*

$$d(P'|P) = (p-1)(d+1).$$

Proof. This is a special case of Proposition III.7.8 in [18]. See Appendix A for more information about the ramification index and the different. □

Definition 2.2.2. *Suppose $y^p - y = f(x)$ defines an Artin-Schreier extension in standard form. For each pole $P_1, \ldots, P_{r+1}$ of $f(x)$, define d_j to be the order of the pole at P_j. The number d_j is the ramification invariant at the point P_j. It can be assumed that $p \nmid d_j$ for all j. For the remainder of the paper, we let $e_j = d_j + 1$.*

Lemma 2.2.3. *Let $y^p - y = f(x)$ define an Artin-Schreier extension in standard form. Suppose $f(x)$ has $r+1$ poles at the points $P_1, \ldots, P_{r+1}$. The genus of the curve $Y : y^p - y - f(x)$ can be expressed in terms of the ramification invariants as follows:*

$$g_Y = \left(\left(\sum_{j=1}^{r+1} e_j \right) - 2 \right) \cdot \frac{p-1}{2}.$$

The formula for the genus follows from the Riemann-Hurwitz formula. To simplify the genus formula, let

$$D + 2 = \sum_{j=1}^{r+1} e_j,$$

then $g_Y = \frac{D(p-1)}{2}$. The number $D+2$ will be used frequently in the Chapter 4.

In the special case where X is an Artin-Schreier curve $X : y^p - y = f(x)$ with $f(x) \in k[x]$, the genus of the curve can be computed using the formula

$$g = \frac{(p-1)(d-1)}{2},$$

where d is the degree of $f(x)$. The following theorem gives a proof about the basis of $H^0(X, \Omega_X^1)$ in this special case.

Proposition 2.2.4. *Let $X : y^p - y = f(x)$ be an Artin-Schreier curve in standard form with $f(x) \in k[x]$ of degree d. A basis for $H^0(X, \Omega^1_X)$ is given by $\{y^r x^b dx\}$ where*

$$0 \leq r \leq p-2 \tag{2.2.1}$$

$$0 \leq b \leq d-2 \tag{2.2.2}$$

$$rd + bp \leq pd - d - p - 1. \tag{2.2.3}$$

Proof. If x is equal to zero, there are p solutions of the equation $y^p - y = f(0)$. Let $R_1, \ldots, R_p$ be the points of X lying above $x = 0$. Then the divisor of the function x is

$$(x) = R_1 + \cdots + R_p - pP_\infty.$$

Let Q_i be the point of X where $y = 0$ and x_i is the ith root of $f(x)$, counted with multiplicity. The function y has a root at each Q_i. The order of the zero of y at Q_i is the order of the root x_i in $f(x)$. The only pole of y is at P_∞. Therefore,

$$(y) = Q_1 + \cdots + Q_d - dP_\infty.$$

The divisor of dx is

$$(dx) = (2g-2)P_\infty = \left(2\frac{(p-1)(d-1)}{2} - 2\right)P_\infty = (pd - d - p - 1)P_\infty.$$

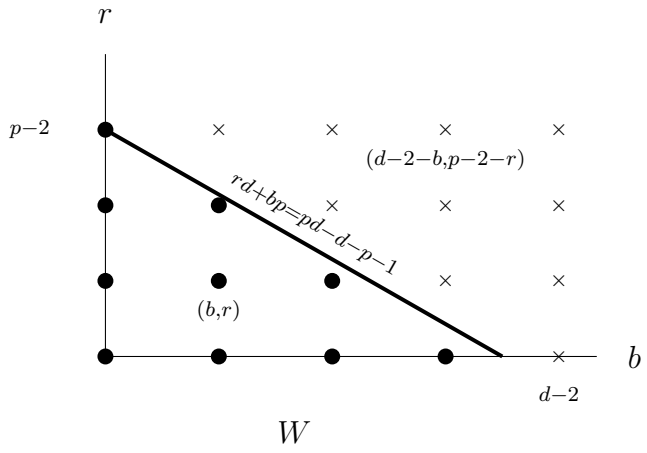
Using the above calculations, we see that the divisor of $x^b y^r dx$ is

$$(x^b y^r dx) = R_1 + \cdots + R_p + Q_1 + \cdots + Q_d - (rd + bp - (pd - d - p - 1))P_\infty.$$

So $x^b y^r dx$ is a holomorphic differential if and only if $rd + bp \leq pd - d - p - 1$. For each pair (b,r) satisfying (2.2.1) and (2.2.2), the number $rd + bp - (pd - d - p - 1)$ will be different because p and d are relatively prime. Therefore, each $x^b y^r dx$ has a different coefficient on P_∞ and we see that this set is linearly independent.

The last thing we need to do is count the number of pairs (b, r) satisfying the conditions stated in the theorem. Ignoring condition (2.2.3), there are $(p-1)(d-1)$ pairs. To see that the genus of X is $(d-1)(p-1)/2$, we need to show that only half

of these points satisfy (2.2.3). We do this by a symmetry argument on pairs (b, r) and $(d-2-b, p-2-r)$. As a visual aid, we provide the following picture for $p = 5$ and $d = 6$.



Let (b, r) be a pair satisfying $rd + bp \leq pd - d - p - 1$. Then

$$(p-2-r)d + (d-2-b)p = 2pd - 2p - 2d - bp - rd. \tag{2.2.4}$$

Using the assumption we made about (b, r), equation (2.2.4) is

$$\begin{aligned} &\geq pd - p - d + 1 \\ &> pd - p - d - 1. \end{aligned}$$

So if (b, r) satisfies (2.2.3), the pair $(d-2-b, p-2-r)$ does not.

Now assume (b, r) is a pair with $rd + bp > pd - d - p - 1$. Then

$$(p-2-r)d + (d-2-b)p = 2pd - 2p - 2d - bp - rd. \tag{2.2.5}$$

Using the assumption we made about (b, r), equation (2.2.5) is

$$< pd - p - d + 1.$$

We need to show that $(p-2-r)d + (d-2-b)p \leq pd - p - d - 1$ but so far we have $(p-2-r)d+(d-2-b)p \leq pd-p-d$. We notice that if $(p-2-r)d+(d-2-b)p = pd-p-d$ then $rd+bp = pd-d-p$. This would mean $(r+1)d+(b+1)p = pd$, which is impossible given conditions (2.2.1) and (2.2.2).

Therefore, the linearly independent set of elements of $H^0(X, \Omega^1_X)$ defined by the conditions in the theorem has $(p-1)(d-1)/2$ elements. Knowing that the genus of this curve is $(p-1)(d-1)/2$, we have found a basis for $H^0(X, \Omega^1_X)$.

□

Proposition 2.2.4 is a special case of the basis given in [19, Lemma 1]. For a more detailed description of the genus, see A.4.

2.3 The p-rank of a curve

Suppose we are given a smooth projective curve X of genus g defined over an algebraically closed field with characteristic $p > 0$. Then X has an associated abelian variety Jac(X) of dimension g called the Jacobian of X, which is an abelian group. To study the Jacobian of X, we look at the multiplication-by-p morphism. The kernel of this map is denoted by Jac$(X)[p]$ and is called the p-torsion of the Jacobian of X. Because the multiplication-by-p morphism is inseparable, Jac$(X)[p]$ has the structure of a group scheme. The group scheme, $\mathbb{G}_m = \text{Spec}(k[x, x^{-1}])$, is called the multiplicative group. Let μ_p be the kernel of Frobenius on $\mathbb{G}_m$. As a scheme, $\mu_p = \text{Spec}(k[x]/(x^p - 1))$. The p-rank of X is $s_X = \dim_{\mathbb{F}_p} \text{Hom}(\mu_p, \text{Jac}(X)[p])$.

The p-torsion points of the Jacobian are the points $Q \in \text{Jac}(X)(k)$ where $pQ = 0$. The set of p-torsion points will be denoted by Jac (X) $[p]$ (k). The number of p-torsion points will be a power of p. The number s_X defined above satisfies

$$\#\text{Jac}\,(X)\,[p]\,(k) = p^{s_X}.$$

The p-rank of a curve satisfies the inequality $0 \leq s_X \leq g$.

Proposition 2.3.1. *Let $X : y^p - y - f(x)$ be an Artin-Schreier curve in standard form and let B be the set of $r+1$ poles of $f(x)$. The p-rank of X is*

$$s_X = r(p-1).$$

The proof of the above proposition is a special case of the Deuring-Shafarevich formula [9].

When the genus of X is one, X is an elliptic curve. In this case, X having p-rank 1 is equivalent to X being an ordinary elliptic curve. If the p-rank of X is 0, this is equivalent to X being a supersingular elliptic curve. We consider this special case further in Appendix B.

2.4 The a-number of an Artin-Schreier curve

The group scheme, $\mathbb{G}_a = \text{Spec}(k[x])$, is called the additive group. Let α_p be the kernel of Frobenius on $\mathbb{G}_a$. As a scheme, $\alpha_p = \text{Spec}(k[x]/(x^p))$. The a-number of X is $a_X = \dim_k \text{Hom}(\alpha_p, \text{Jac}(X)[p])$.

The a-number of a curve is bounded by zero and the genus of the curve. If the p-rank is not equal to the genus, then the a-number is strictly greater than zero. If the a-number is equal to g, then the Jacobian of the curve is isomorphic to a product of supersingular elliptic curves.

2.5 The Cartier operator and the a-number

The Cartier operator, $\mathcal{C}$, gives a semi-linear map $\mathcal{C} : H^0(X, \Omega^1_X) \to H^0(X, \Omega^1_X)$ with the following properties (see [5]):

- $\mathcal{C}(\omega_1 + \omega_2) = \mathcal{C}(\omega_1) + \mathcal{C}(\omega_2)$
- $\mathcal{C}(f^p \omega) = f\mathcal{C}(\omega)$
- $\mathcal{C}(f^{n-1} df) = \begin{cases} df & \text{if } n = p, \\ 0 & \text{if } 0 < n < p. \end{cases}$

Suppose $\beta = \{\omega_1, \ldots, \omega_g\}$ is a basis of $H^0(X, \Omega^1_X)$. For each ω_j, write

$$\mathcal{C}(\omega_j) = \sum_i m_{i,j}\, \omega_i.$$

The matrix M with entries $(m_{i,j})^p$ is the $g \times g$ **Cartier-Manin matrix** of the curve X with respect to β. The a**-number** of the curve X is

$$a_X = g - \text{rank}(M).$$

2.6 Example of a family of Artin-Schreier curves where the a-number is constant

Let $p = 5$. In this section, we show that any Artin-Schreier curve $y^5 - y = f(x)$, where $f(x) \in k[x]$ has degree 4, has a-number 4. If the Artin-Schreier curve is in standard form, it is given by an affine equation $X : y^5 - y = x^4 + a_2x^2 + a_1x$. A basis of $H^0(X, \Omega^1_X)$ is given by the set $\{dx, xdx, x^2dx, ydx, yxdx, y^2dx\}$. In this case, the genus of X is $g = 6$. Applying the Cartier operator to each element of our basis, we get:

$$\begin{aligned}
\mathcal{C}(dx) &= 0.\\
\mathcal{C}(xdx) &= 0.\\
\mathcal{C}(x^2dx) &= 0.\\
\mathcal{C}(ydx) &= \mathcal{C}((y^5 - x^4 - a_2x^2 - a_1x)dx)\\
&= \mathcal{C}(-x^4dx)\\
&= 4dx.\\
\mathcal{C}(yxdx) &= \mathcal{C}\left((y^5 - x^4 - a_2x^2 - a_1x)xdx\right)\\
&= 0.\\
\mathcal{C}(y^2dx) &= \mathcal{C}\left((y^5 - x^4 - a_2x^2 - a_1x)^2dx\right)
\end{aligned}$$

$$= \mathcal{C}(-2x^4y^5) + \mathcal{C}(a_2^2x^4dx)$$
$$= 3ydx + (a_2^2)^{1/5}dx$$

This gives the Cartier-Manin matrix:

$$M = \begin{pmatrix} 0 & 0 & 0 & 4 & 0 & a_2^2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

This matrix has rank 2. So, any Artin-Schreier curve given by a degree four polynomial $f(x)$ has a-number $a_X = g - \text{rank}(M) = 6 - 2 = 4$.

2.7 Some results related to the a-number

In [4], it is shown that if the genus of a curve is $g > \frac{p(p-1)}{2}$ then $a_X \neq g$.

Theorem 2.7.1. *(Ekedahl) Let g denote the genus of a curve X defined over k. The Jacobian of X is not isomorphic to a product of supersingular elliptic curves, i.e., $a_X \neq g$ if*

1. $g > \frac{p(p-1)}{2}$
2. $g > \frac{p-1}{2}$ *if X is hyperelliptic and* $(p, g) \neq (2, 1)$.

We will explore this result for Artin-Schreier curves given by affine equation $y^p - y = f(x)$ with $f(x) \in k[x]$ in two ways. First, we give a proof of part 1 of Theorem 2.7.1 for $p \geq 3$. Second, we give an example to show that this result is optimal.

Proof. Suppose X is an Artin-Schreier curve with affine equation $y^p - y = f(x)$ with $f(x) \in k[x]$. Recall that the genus of this curve is given by $g = (\deg f(x) - 1)(p-1)/2$.

Since we are assuming that $g > p(p-1)/2$, we must have that $\deg f(x) \geq p+2$. With this fact, we can show that the 1-form $x^{p-1}dx$ is in $H^0(X, \Omega_X^1)$. This requires showing that the equation

$$rd + bp \leq pd - d - p - 1$$

is satisfied when $r = 0$ and $b = p-1$. Using that $\deg f(x) \geq p+2$, the right hand side of this inequality is greater than or equal to $p^2 - 3$. The left hand side is equal to $p^2 - p$. Since $p \geq 3$, we have that $rd + bp \leq pd - d - p - 1$. So, $x^{p-1}dx$ is in $H^0(X, \Omega_X^1)$.

The Cartier operator applied to $x^{p-1}dx$ yields $\mathcal{C}(x^{p-1}dx) = dx$. This means that the rank of the Cartier-Manin matrix must be at least one because it has an entry corresponding to this calculation. Therefore, the a-number of X cannot equal g. □

To see that that the result of [4] is optimal, consider the curve $X : y^p - y = x^{p+1}$. We will show the well known result that $a_X = g$ for this curve by showing that the image of $\mathcal{C}$ on all 1-forms is 0.

Theorem 2.7.2. *The a-number of the Artin-Schreier curve $X : y^p - y = x^{p+1}$ is*

$$a_C = g = \frac{p(p-1)}{2}.$$

Proof. The basis for $H^0(X, \Omega_X^1)$ we will use is given by $\{y^r x^b dx\}$ with the three conditions given in Proposition 2.2.4. Using $d = p+1$, and equations (2.2.1),(2.2.2) and (2.2.3) gives

$$0 \leq b \leq p-2$$

$$0 \leq r \leq p-1$$

$$b \leq p - 1 - r - \frac{r+2}{p}.$$

Notice that $\mathcal{C}(x^b dx) = 0$ for all b because $0 \leq b \leq p-2$. Now consider $\mathcal{C}(x^b y^r dx)$:

$$\begin{aligned}
&\mathcal{C}(x^b y^r dx) \\
&= \mathcal{C}\left(x^b \left(y^p - x^{p+1}\right)^r dx\right) \\
&= \mathcal{C}(x^b(y^{rp} - rx^{(p+1)}y^{(r-1)p} + rx^{2(p+1)}y^{(r-2)p} + \dots \\
&\quad + (-1)^{r-1}rx^{(r-1)(p+1)}y^p + (-1)^r x^{r(p+1)})dx) \\
&= \mathcal{C}((x^b y^{rp} - rx^{(p+1)}x^b y^{(r-1)p} + rx^{2(p+1)}x^b y^{(r-2)p} + \dots \\
&\quad + (-1)^{r-1}rx^{(r-1)(p+1)}x^b y^p + (-1)^r x^{r(p+1)}x^b)dx)
\end{aligned}$$

Let's look at the exponents on x in the above calculation:

$$\begin{aligned}
&x^b \\
&x^{p+1}x^b = x^{p+1+b} \\
&x^{2p+2}x^b = x^{2p+2+b} \\
&x^{3p+3}x^b = x^{3p+3+b} \\
&\vdots \\
&x^{rp+r}x^b = x^{rp+r+b}
\end{aligned}$$

We will show that none of the exponents above are congruent to $-1 \bmod p$ and thus $\mathcal{C}(x^b y^r dx) = 0$. Suppose $ap + a + b = (a+1)p - 1$ where $0 \leq a \leq r$. This gives $b = p - a - 1$. From above, we know that $b \leq p - 1 - r - \frac{r+2}{p}$, giving a contradiction. Thus, $\mathcal{C}(x^b y^r dx) = 0$ for all possible b and r. □

The result of [4] was given for all nonsingular curves. In [5], the focus is on cyclic covers of the projective line. In particular, this paper gives lower bounds on the a-number of cyclic covers $X : y^\ell = f(x)$ with $f(x) \in k[x]$. We give the main result of [5] below.

Theorem 2.7.3. *(Elkin) Let k be an algebraically closed field of characteristic $p > 0$ and $\ell \neq p$ be prime. Let $X : y^\ell = f(x)$ be a curve defined by $f(x) \in k[x]$, where $f(x)$ has no repeated roots, of genus g.*

1. *If* $\ell = 2$, $a_X \leq (1 - 2/p)g + (p-1)/p$.

2. *If* $2 < \ell < p$, $a_X \leq (1 - 2/p)g + 2(\ell - 1)(p-1)/p$.

3. *If* $\ell > p$, $a_X < (1 - 2(1-u)/p)g + (\ell - 1)(2p - 2 + u)/p$
   where $u = (\ell + p - 1)/2\ell p$.

The main result of this paper is closely related to the results of [14]. In [14], a formula is given for the a-number of Artin-Schreier curves of the form $X : y^p - y = x^d$ for all $d > 0$.

Theorem 2.7.4. *(Pries) Let* a_X *be the* a*-number of the curve* $y^p - y = x^d$.

1. *If* $p \equiv 1 \bmod d$, *then*

$$a_X = \begin{cases} \frac{(p-1)d}{4} & \text{if } d \text{ even} \\ \frac{(p-1)(d-1)(d+1)}{4d} & \text{if } d \text{ odd.} \end{cases}$$

2. *If* $p \not\equiv 1 \bmod d$, *define* $h_b \in [0, p-1]$ *to be the integer satisfying* $h_b \equiv (-1-b)d^{-1} \bmod p$. *Then*

$$a_X = \sum_{b=0}^{d-2} \mathit{min}\left(h_b, p - \lceil (p + 1 + bp)/d \rceil\right).$$

We extend the result of part (1) to all curves $X : y^p - y = f(x)$, with $f(x) \in k(x)$ whose poles have order dividing $p - 1$, in chapter 3.

Chapter 3

Main result

The result in this chapter was discovered by using a computer to compute the a-number of Artin-Schreier curves $y^p - y = f(x)$ with $f(x) \in \mathbb{F}_p[x]$. We used the computer algebra system Maple to compute the a-number for a given prime p and polynomial $f(x)$. Letting Maple produce random polynomials, $f(x)$, led to the discovery of the main result of the paper. This code is included in Appendix C.

Let k be an algebraically closed field of characteristic p. In this section, we consider an Artin-Schreier curve of the form $X : y^p - y = f(x)$ with $f(x) \in k(x)$ satisfying that $f(x) \neq z^p - z$ for any $z \in k(x)$. After a fractional linear transformation, we can suppose that $f(x)$ has a pole at infinity. Taking the partial fraction decomposition of $f(x)$, we can write

$$f(x) = f_0(x) + \sum_{j=1}^{\mu} f_j \left(\frac{1}{x - e_j} \right)$$

where, for each $0 \leq j \leq \mu$, $f_j \in k[x]$ is a polynomial. Defining

$$x_j = \begin{cases} x & \text{if } j = 0, \\ (x - e_j)^{-1} & \text{if } j \in \{1, \ldots, \mu\}, \end{cases}$$

we can write

$$f(x) = \sum_{j=0}^{\mu} f_j \left(x_j \right).$$

Let d_j and δ_j be the degree and leading coefficient of the polynomial f_j, respectively. We consider the situation where the order of each pole of $f(x)$ divides the quantity $(p-1)$, i.e., each d_j divides $(p-1)$. As each d_j divides $(p-1)$, we will define the integers $\gamma_j = \frac{p-1}{d_j}$.

Theorem 3.1. *With the setup as above, the a-number of the Artin-Schreier curve* $X : y^p - y = f(x)$ *is*

$$a_X = \sum_{j=0}^{\mu} a_j, \text{ where}$$

$$a_j = \begin{cases} \frac{(p-1)d_j}{4} & \text{if } d_j \text{ even} \\ \frac{(p-1)(d_j-1)(d_j+1)}{4d_j} & \text{if } d_j \text{ odd.} \end{cases}$$

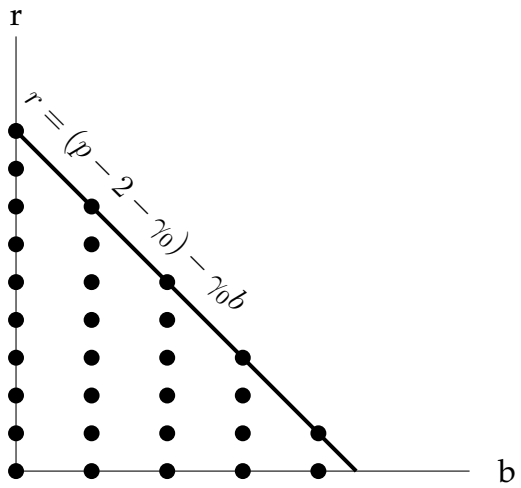
Proof. We will use the basis for $H^0(X, \Omega^1_X)$ given by [19, Lemma 1]. This basis is given by the set $W = \cup_{j=0}^{\mu} W_j$ where

$$W_0 = \left\{ x^b y^r dx \middle| r, b \geq 0 \text{ and } rd_0 + bp \leq (p-1)(d_0-1) - 2 \right\}, \text{ and}$$

$$W_j = \left\{ x_j^b y^r dx \middle| r \geq 0, b \geq 1, \text{ and } rd_j + bp \leq (p-1)(d_j+1) \right\} \text{ if } j \neq 0.$$

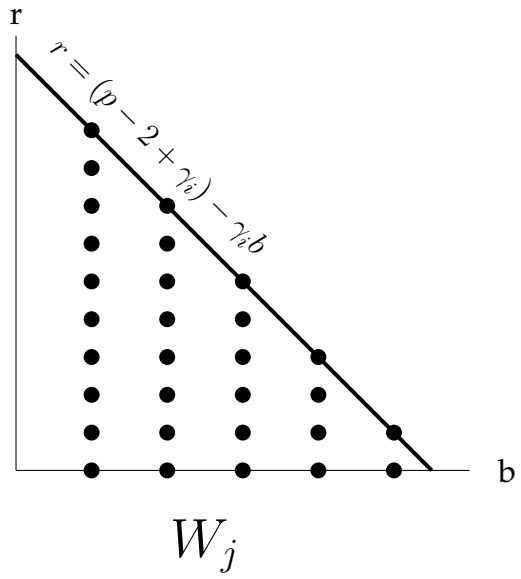
We note that $|W_0| = (d_0-1)(p-1)/2$, and $|W_j| = (d_j+1)(p-1)/2$.

The set of 1-forms $x^b y^r dx \in W_0$ can be associated with the integer ordered pairs (b, r) that lie in the region bounded by the lines $r = 0, b = 0$, and $r = (p-2-\gamma_0) - \gamma_0 b$.



W_0

Similarly, the 1-forms $x_j^b y^r dx \in W_j$ can be associated with the integer pairs (b, r) lying in the region bounded by $r = 0$, $b = 1$, and $r = (p - 2 + \gamma_j) - \gamma_j b$.



We define an ordering $\prec$ on the basis W. Define $x_i^{b_1} y^{r_1} dx \prec x_j^{b_2} y^{r_2} dx$ if

1. $r_1 < r_2$, or if
2. $r_1 = r_2$ and $i < j$, or if
3. $r_1 = r_2$, $i = j$ and $b_1 < b_2$.

This gives W the following ordering.

$$W = \Big\{ dx, xdx, x^2dx, \ldots, x_1dx, x_1^2dx, \ldots, x_\mu dx, x_\mu^2 dx, \ldots$$
$$ydx, xydx, x^2ydx, \ldots, x_1ydx, x_1^2ydx, \ldots, x_\mu ydx, x_\mu^2 ydx, \ldots \Big\}$$

We now consider the action of the Cartier operator on the elements of the set W_j for a fixed j. In general,

$$\mathcal{C}\left(x_j^b y^r dx\right) = \mathcal{C}\left(x_j^b \left(y^p - f(x)\right)^r dx\right)$$

Using the extended binomial theorem,

$$(y^p - f(x))^r = \sum_{\substack{(\alpha_{-1},\ldots,\alpha_\mu) \\ \sum_i \alpha_i = r}} c_\alpha y^{p\alpha_{-1}} f_0^{\alpha_0}(x) f_1^{\alpha_1}(x_1) \cdots f_\mu^{\alpha_\mu}(x_\mu)$$

where $\alpha = (\alpha_{-1}, \ldots, \alpha_\mu)$ and $c_\alpha = (-1)^{\alpha_0+\cdots+\alpha_\mu}\binom{r}{\alpha_0,\ldots,\alpha_\mu}$. So,

$$\mathcal{C}\left(x_j^b y^r dx\right) = \sum_{\substack{(\alpha_{-1},\ldots,\alpha_\mu) \\ \sum_i \alpha_i = r}} c_\alpha y^{\alpha_{-1}} \mathcal{C}\left(x_j^b f_0^{\alpha_0}(x) f_1^{\alpha_1}(x_1) \cdots f_\mu^{\alpha_\mu}(x_\mu)\, dx\right)$$

Lemma 1. *If $r \geq (b+1)\gamma_0$, then the 1-form $x^b y^{r-(b+1)\gamma_0} dx$ appears in the expansion of $\mathcal{C}(x^b y^r dx)$.*

Proof. Consider the terms of

$$\mathcal{C}\left(x^b y^r dx\right) = \sum_{\substack{(\alpha_{-1},\ldots,\alpha_\mu) \\ \sum_i \alpha_i = r}} c_\alpha y^{\alpha_{-1}} \mathcal{C}\left(x_j^b f_0^{\alpha_0}(x) f_1^{\alpha_1}(x_1) \cdots f_\mu^{\alpha_\mu}(x_\mu)\, dx\right)$$

where $\alpha_{-1} = r - (b+1)\gamma_0$. The biggest choice for α_0 is then $(b+1)\gamma_0$. For this choice of α, i.e., $\alpha = (r - (b+1)\gamma_0, (b+1)\gamma_0, 0, \ldots, 0)$, the term of the above sum becomes

$$c_\alpha y^{r-(b+1)\gamma_0} \mathcal{C}\left(x^b f_0^{(b+1)\gamma_0}(x) dx\right) = c_\alpha y^{r-(b+1)\gamma_0}\left(\delta_{0,d_j}^{(b+1)\gamma_0/p} x^b + \ldots\right) dx$$

as $\deg\left(x^b f_0^{(b+1)\gamma_0}(x)\right) = b + (b+1)\gamma_0 d_0 = (b+1)p - 1$.

To show that the coefficient of $y^{r-(b+1)\gamma_0} x^b$ on the right hand side of the above equation is nonzero, we notice that for all $x^b y^r dx \in W_0$, we have $r \leq p - 2 - \gamma_0$. This fact gives that $c_\alpha \neq 0$. Also, as δ_{0,d_j} is the leading coefficient of f_0, we have that $\delta_{0,d_j} \neq 0$.

To show that this term is canceled by no others, we note that no other choice for α_{-1} would yield the correct power on y. We also note that any smaller choice for α_0 would not give a high enough power to yield x^b. Thus, the 1-form $x^b y^{r-(b+1)\gamma_0} dx$ appears in the expansion of $\mathcal{C}(x^b y^r dx)$.

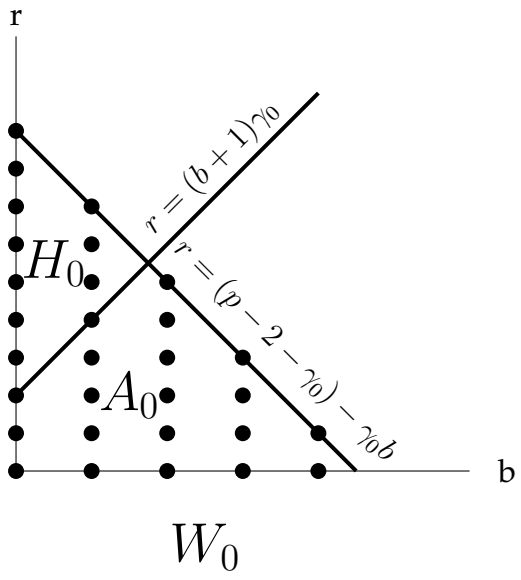
□

We partition W_0 into two subsets, those elements which satisfy the hypothesis of Lemma 1 and those that do not. We call these subsets H_0 and A_0, respectively. That is,

$$H_0 = \left\{ x^b y^r dx \in W_0 | r \geq (b+1)\gamma_0 \right\},$$

and

$$A_0 = W_0 - H_0.$$



Lemma 2. *For $1 \leq j \leq \mu$, if $r \geq (b-1)\gamma_j$, then the 1-form $x_j^b y^{r-(b-1)\gamma_j} dx$ appears in the expansion of $\mathcal{C}(x_j^b y^r dx)$.*

Proof. If $r \geq (b-1)\gamma_j$, we see that the term of $\mathcal{C}\left(x_j^b y^r dx\right)$ where $\alpha_{-1} = r - (b-1)\gamma_j$, $\alpha_j = (b-1)\gamma_j$, and $\alpha_i = 0$ for all $i \notin \{-1, i\}$ is

$$c_\alpha y^{r-(b-1)\gamma_j} \mathcal{C}\left(x_j^b f_j \left(x_j\right)^{(b-1)\gamma_j}\right) = c_\alpha \delta_{j,d_j}^{(b-1)\gamma_j/p} x_j^b y^{r-(b-1)\gamma_j} dx + \ldots \tag{3.1}$$

because the term in the denominator of $x_j^b f_j \left(x_j\right)^{(b-1)\gamma_j}$ with the largest exponent is $(x - e_j)^{(b-1)\gamma_j d_j + b} = (x - e_j)^{(b-1)p+1}$.

To show that the coefficient of the term shown on the right hand side of (3.1) is nonzero, we note that for all $x_j^b y^r \in W_j$, we have $r \leq p-2$. This gives that $c_\alpha \neq 0$. Also, $\delta_{j,d_j} \neq 0$ as it is the leading coefficient of f_j.

The term on the right hand side of (3.1) cannot be canceled by another term in the expansion of $\mathcal{C}(x_j^b y^r dx)$. To see this, we notice that in order for $x_j^b y^{r-(b-1)\gamma_j} dx$ to appear, we must have $\alpha_{-1} = r - (b-1)\gamma_j$. But if a_j is chosen any smaller than $(b-1)\gamma_j$, as it was chosen above, the 1-form $x_j^b y^{r-(b-1)\gamma_j} dx$ will not appear in the expansion of $\mathcal{C}(x_j^b y^r dx)$.

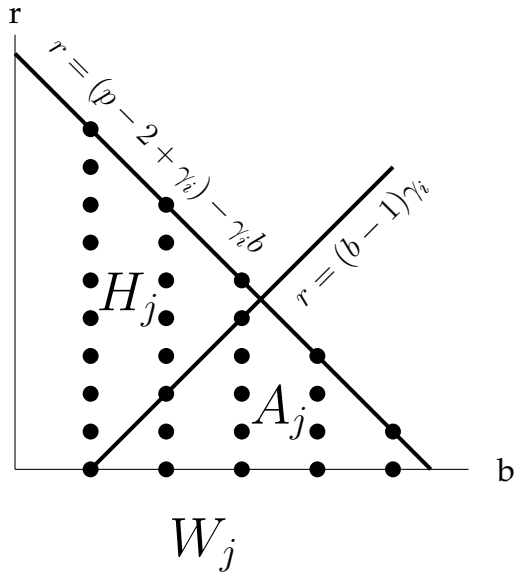
□

Based on the hypothesis of Lemma 2, we partition the set W_j into two subsets, H_j and A_j. Let

$$H_j = \left\{ x_j^b y^r dx \in W_j \middle| r \geq (b-1)\gamma_j \right\},$$

and

$$A_j = W_j - H_j.$$



For convenience, we define the sets

$$H = \cup_{j=0}^{\mu} H_j$$

and

$$A = \cup_{j=0}^{\mu} A_j.$$

Based on the statements of Lemma 1 and Lemma 2, we make the following definition for the 1-forms in H_j. We will say that the **key term** of $\mathcal{C}(\omega)$ is

$$\begin{cases} x^b y^{r-(b+1)\gamma_0} dx & \text{if } \omega = x^b y^r dx \in H_0, \\ x_j^b y^{r-(b-1)\gamma_j} dx & \text{if } \omega = x_j^b y^r dx \in H_j \text{ for some } j \neq 0. \end{cases}$$

We note that Lemmas 1 and 2 guarantee a key term to appear in the expansion of ω for all $\omega \in H$. The next Lemma will show that this key term does not appear for any basis element smaller than ω. Lemmas 1-3 show that the columns of the Cartier-Manin matrix which correspond to H are linearly independent.

Lemma 3. *1. The 1-form $x^b y^{r-(b+1)\gamma_0} dx$ does not appear in the expansion of $\mathcal{C}(\omega)$ for any $\omega \prec x^b y^r dx$.*

2. The 1-form $x_j^b y^{r-(b-1)\gamma_j} dx$ does not appear in the expansion of $\mathcal{C}(\omega)$ for any $\omega \prec x_j^b y^r dx$.

Proof.

To show that (1) is true, we will show that $x^b y^{r-(b+1)\gamma_0} dx$ can only appear in the expansion of $\mathcal{C}(\omega)$ if $\omega \geq x^b y^r dx$. Recall the calculation

$$\mathcal{C}\left(x_k^B y^R dx\right) = \sum_{\substack{(\alpha_{-1},\ldots,\alpha_\mu) \\ \sum_i \alpha_i = R}} c_\alpha y^{\alpha_{-1}} \mathcal{C}\left(x_k^B f_0^{\alpha_0}(x) f_1^{\alpha_1}(x_1) \cdots f_\mu^{\alpha_\mu}(x_\mu)\right).$$

In order for $x^b y^{r-(b+1)\gamma_0} dx$ to appear in the expansion of $\mathcal{C}\left(x_k^B y^R dx\right)$, we need $\alpha_{-1} = r - (b+1)\gamma_0$. This gives the restriction that $\alpha_0 \leq R - (r - (b+1)\gamma_0)$. At this point, we must consider two cases: when $k = 0$ and when $k \neq 0$.

If $k = 0$, we need $\alpha_0 d_0 + B \geq (b+1)p - 1$ in order for $x^b y^{r-(b+1)\gamma_0} dx$ to appear in the expansion of $\mathcal{C}\left(x^B y^R dx\right)$. Combining these inequalities, we find that

$$R - r \geq \frac{b - B}{d_0}.$$

Using that $0 \leq b, B \leq d_0 - 2$, we have that the 1-form $x^b y^{r-(b+1)\gamma_0} dx$ can appear in the expansion of $\mathcal{C}\left(x^B y^R dx\right)$ only if $R > r$ or if $R = r$ and $B \geq b$.

If $k \neq 0$, we require $\alpha_0 d_0 - B \geq (b+1)p - 1$ in order for $x^b y^{r-(b+1)\gamma_0} dx$ to appear in the expansion of $\mathcal{C}\left(x_k^B y^R dx\right)$. Performing a similar calculation to the one in the previous case, we find that

$$R - r \geq \frac{b+B}{d_0}.$$

As $B > 0$, we conclude that $x^b y^{r-(b+1)\gamma_0} dx$ can only appear in the expansion of $\mathcal{C}\left(x_k^B y^R dx\right)$ if $R > r$. In both cases, we have shown that $x_k^B y^R dx$ must be greater than or equal to $x^b y^r dx$. This finishes the proof of part (1).

To prove part (2), we must show that $x_j^b y^{r-(b-1)\gamma_j} dx$ can only appear in the expansion of $\mathcal{C}(\omega)$ if $\omega \geq x_j^b y^r dx$.

We will once again need to look at the calculation

$$\mathcal{C}\left(x_k^B y^R dx\right) = \sum_{\substack{(\alpha_{-1},\ldots,\alpha_\mu) \\ \sum_i \alpha_i = R}} c_\alpha y^{\alpha_{-1}} \mathcal{C}\left(x_k^B f_0^{\alpha_0}(x) f_1^{\alpha_1}(x_1) \cdots f_\mu^{\alpha_\mu}(x_\mu)\right).$$

We see that we need $\alpha_{-1} = r - (b-1)\gamma_j$ in order for $x_j^b y^{r-(b-1)\gamma_i} dx$ to appear in the output of $\mathcal{C}\left(x_k^B y^R dx\right)$. This gives the restriction that $\alpha_j \leq R - (r - (b-1)\gamma_j)$.

If $k \neq j$, we see that $x_j^b y^{r-(b-1)\gamma_j} dx$ will only show up in the expansion of $\mathcal{C}\left(x_k^B y^R dx\right)$ if $\alpha_j d_j \geq (b-1)p + 1$. Using the inequalities above we see that

$$R - r \geq \frac{b}{d_j}.$$

As $b > 0$, we conclude that $x_j^b y^{r-(b-1)\gamma_j} dx$ can only appear in the expansion of $\mathcal{C}\left(x_k^B y^R dx\right)$ if $R > r$.

If $k = j$, we need $\alpha_j d_j + B \geq (b-1)p + 1$ for $x_j^b y^{r-(b-1)\gamma_i} dx$ to appear in the expansion of $\mathcal{C}\left(x_j^B y^R dx\right)$. Using the inequalities above, we find that

$$R - r \geq \frac{b-B}{d_j}. \tag{3.2}$$

Using that b and B are both bounded by d_j, we see that this equation is only satisfied if $R > r$ or if $R = r$ and $B \geq b$. This completes the proof of statement (2).

□

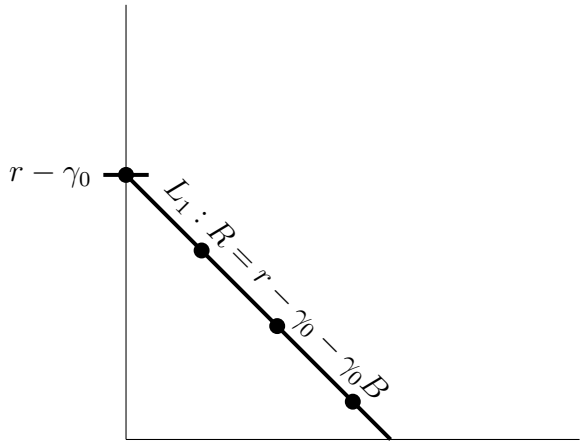
Recall the definition of the key terms for $\omega \in H_j$. The key term of $\mathcal{C}\left(x^b y^r dx\right)$ is

$$x^b y^{r-(b+1)\gamma_0} dx, \tag{3.3}$$

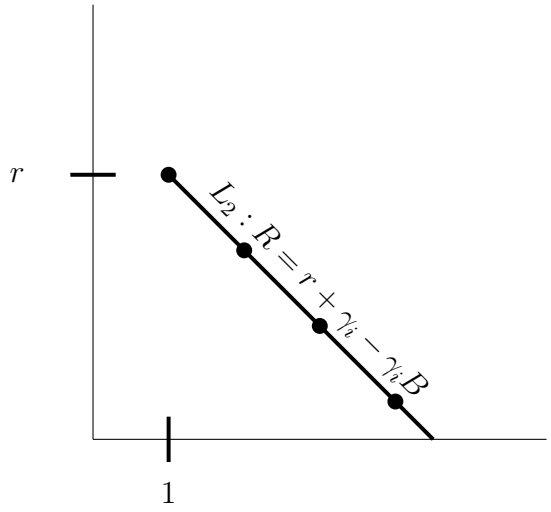
and the key term of $\mathcal{C}\left(x_j^b y^r dx\right)$ is

$$x_j^b y^{r-(b-1)\gamma_j} dx \tag{3.4}$$

First, consider the term in (3.3) for a fixed r as b increases from zero. These terms lie on a line of slope $-\gamma_0$ as shown on the following graph.



The term shown in (3.4) can be thought of in a similar way. Here, the terms shown in (3.4) appear on a line of slope $-\gamma_i$ as shown below.



With these two pictures in mind, we make the following definitions. First, let

$$Z_{0,r} = \left\{ x^B y^R dx \in W_0 \middle| R = r - \gamma_0 - \gamma_0 B \right\} \text{ if } i = 0, \text{ and}$$
$$Z_{j,r} = \left\{ x_j^B y^R dx \in W_j \middle| R = r + \gamma_j - \gamma_j B \right\} \text{ if } j \in \{1, \ldots, \mu\}.$$

Second, let

$$Y_{j,r} = \begin{cases} \cup_{i=\gamma_0}^{r} Z_{0,i} & \text{if } j = 0, \\ \cup_{i=0}^{r} Z_{j,i} & \text{if } j \in \{1, \ldots, \mu\}. \end{cases}$$

We now turn our attention to showing that the columns of the Cartier-Manin matrix that correspond to the basis elements in A are linearly dependent on the columns corresponding to the set H. The following two lemmas will show that the output of the Cartier operator is contained in the span of the sets $Y_{i,r}$. As the sets $Y_{i,r}$ are built from key terms, which come from the image of the Cartier operator on H, we will have that each term in the output of the Cartier operator on an element of A also appears as a key term for some element of H.

Lemma 4. *If $\omega \in W_j$ appears in the expansion of $\mathcal{C}\left(x_j^b y^r dx\right)$ then $\omega \in Y_{j,r}$.*

Proof. The proof will be in two parts. First, we will show this statement when $j = 0$. In order to show this, we will show that if the inequality $R \geq r - \gamma_0 - \gamma_0 B + 1$ holds

then $x^B y^R dx$ will not appear as a term of $\mathcal{C}\left(x^b y^r dx\right)$. Recall that

$$\mathcal{C}\left(x^b y^r dx\right) = \sum_{\substack{(\alpha_{-1},\ldots,\alpha_\mu) \\ \sum_i \alpha_i = r}} c_\alpha y^{\alpha_{-1}} \mathcal{C}\left(x^b f_0^{\alpha_0}(x) f_1^{\alpha_1}(x_1) \cdots f_\mu^{\alpha_\mu}(x_\mu)\right).$$

For $x^B y^R dx$ to appear in the expansion, we must have $\alpha_{-1} = R$. This gives that $\alpha_0 \leq r - R$. Now using that $R \geq r - \gamma_0 - \gamma_0 B + 1$, we have $\alpha_0 \leq \gamma_0 B + \gamma_0 - 1$. We now notice that the degree of $x^b f_0^{\alpha_0}$ is

$$\begin{aligned}
\deg\left(x^b f_0^{\alpha_0}\right) &= b + \alpha_0 d_0 \\
&\leq b + \left(\gamma_0 B + \gamma_0 - 1\right) d_0 \\
&= b + (p-1)B + (p-1) - d_0 \\
&= (B+1)p - 1 - B + b - d_0.
\end{aligned}$$

By looking at the picture of W_0, we see that $b \leq d_0 - 2$. So, $\deg\left(x^b f_0^{\alpha_0}\right) < (B+1)p - 1$. Thus, $x^B y^R dx$ does not appear as a term in the expansion of $\mathcal{C}\left(x^b y^r dx\right)$ with $R > r - \gamma_0 - \gamma_0 B$.

We now prove the claim in the case when $j \neq 0$. Here, the claim can be restated in the following way. There is no term $x_j^B y^R dx$ appearing in the expansion of $\mathcal{C}\left(x_j^b y^r dx\right)$ with $R > r + \gamma_j - \gamma_j B$. We will use the inequality $R \geq r + \gamma_j - \gamma_j B + 1$. Recall that

$$\mathcal{C}\left(x_j^b y^r dx\right) = \sum_{\substack{(\alpha_{-1},\ldots,\alpha_\mu) \\ \sum_i \alpha_i = r}} c_\alpha y^{\alpha_{-1}} \mathcal{C}\left(x_j^b f_0^{\alpha_0}(x) f_1^{\alpha_1}(x_1) \cdots f_\mu^{\alpha_\mu}(x_\mu)\right).$$

For $x_j^B y^R dx$ to appear as a term in the expansion, we must have $\alpha_{-1} = R$. This gives that $\alpha_j \leq r - R$. Now using that $R \geq r + \gamma_j - \gamma_j B + 1$, we have $\alpha_j \leq \gamma_j B - \gamma_j - 1$. We now notice that the degree of $x_j^b f_j^{\alpha_j}$ is

$$\begin{aligned}
\deg\left(x_j^b f_j^{\alpha_j}\right) &= \alpha_j d_j + b \\
&\leq \left(\gamma_j B - \gamma_j - 1\right) d_j + b \\
&= (p-1)B - (p-1) - d_j + b \\
&= (B-1)p + 1 - B - d_j + b.
\end{aligned}$$

Looking at the picture of W_j we see that $b \leq d_j$. As B has to be greater than or equal to one, we see that $\deg\left(x_j^b f_j^{\alpha_j}\right) < (B-1)p+1$. Thus, $x_j^B y^R dx$ does not appear as a term in the expansion of $\mathcal{C}\left(x_j^b y^r dx\right)$ if $R > r + \gamma_j - \gamma_j B$.

□

Lemma 5. *If $\omega \in W_j$ appears in the expansion of $\mathcal{C}\left(x_i^b y^r dx\right)$, where $i \neq j$, then $\omega \in Y_{j,r-1}$.*

Proof. This claim will be proven in two parts. First, when $j \neq 0$ and $i \neq j$, we can restate the claim in the following way. The term $x_j^B y^R dx$ does not appear as a term in the expansion of $\mathcal{C}\left(x_i^b y^r dx\right)$ where $R \geq r + \gamma_j - \gamma_j B$.

Assume that $R \geq r + \gamma_j - \gamma_j B$. Then

$$\mathcal{C}\left(x_i^b y^r dx\right) = \sum_{\substack{(\alpha_{-1},\ldots,\alpha_\mu) \\ \sum_i \alpha_i = r}} c_\alpha y^{\alpha_{-1}} \mathcal{C}\left(x_i^b f_0^{\alpha_0}(x) f_1^{\alpha_1}(x_1) \cdots f_\mu^{\alpha_\mu}(x_\mu)\right).$$

For $x_j^B y^R dx$ to appear as a term in the expansion, we must have $\alpha_{-1} = R$. This gives that $\alpha_j \leq r - R$. Now using that $R \geq r + \gamma_j - \gamma_j B$, we have $\alpha_j \leq \gamma_j B - \gamma_j$. We notice that in the argument of $c_\alpha y^R \mathcal{C}(x_i^b f_0^{\alpha_0}(x) f_1^{\alpha_1}(x_1) \cdots f_\mu^{\alpha_\mu}(x_\mu))$, the degree of x_j is less than or equal to $\alpha_j d_j$, which is less than $(B-1)p+1$. Thus, $x_j^B y^R dx$ does not appear as a term in the expansion of $\mathcal{C}\left(x_i^b y^r dx\right)$ if $R \geq r + \gamma_j - \gamma_j B$.

The next case to consider is when $j = 0$ and $i \neq 0$. Here, the claim states that there is no term $x^B y^R dx$ appearing in the expansion of $\mathcal{C}\left(x_i^b y^r dx\right)$ with $R \geq r - \gamma_0 - \gamma_0 B$.

Assume that $R \geq r - \gamma_0 - \gamma_0 B$. In the calculation of

$$\mathcal{C}\left(x_i^b y^r dx\right) = \sum_{\substack{(\alpha_{-1},\ldots,\alpha_\mu) \\ \sum_i \alpha_i = r}} c_\alpha y^{\alpha_{-1}} \mathcal{C}\left(x_i^b f_0^{\alpha_0}(x) f_1^{\alpha_1}(x_1) \cdots f_\mu^{\alpha_\mu}(x_\mu)\right),$$

we would need $\alpha_{-1} = R$ in order for $x^B y^R dx$ to appear in the output. This, together with the inequality $R \geq r - \gamma_0 - \gamma_0 B$, gives that $\alpha_0 \leq \gamma_0 B + \gamma_0$. We now see that in the argument of $c_\alpha y^{\alpha_{-1}} \mathcal{C}\left(x_i^b f_0^{\alpha_0}(x) f_1^{\alpha_1}(x_1) \cdots f_\mu^{\alpha_\mu}(x_\mu)\right)$, the degree of x is less than or equal to $\alpha_0 d_0$, which is less than $(B+1)p+1$. Thus, $x^B y^R dx$ does not appear as a term in the expansion of $\mathcal{C}\left(x_i^b y^r dx\right)$ if $R \geq r - \gamma_0 - \gamma_0 B$.

□

Lemmas 3, 4, and 5 show that the Cartier operator applied to $x^b y^r dx$ or $x_j^b y^r dx$ can be written in the following way. If $x^b y^r dx \in W_0$ then

$$\mathcal{C}\left(x^b y^r dx\right) = \nu_{0,b,r-\gamma_0-b\gamma_0} x^b y^{r-\gamma_0-b\gamma_0} dx + \nu_{0,b-1,r-b\gamma_0} x^{b-1} y^{r-b\gamma_0} dx + \cdots + \nu_{0,0,r-\gamma_0} y^{r-\gamma_0} dx + \sum_{k=0}^{\mu} \left(\sum_{R<r+\gamma_k-\gamma_k B} \nu_{k,B,R} x_k^B y^R dx \right) \tag{3.5}$$

where each $\nu_{k,b,r} \in k$ and $\nu_{0,b,r-\gamma_0-b\gamma_0} \neq 0$. If $x_j^b y^r dx \in W_j$ then

$$\mathcal{C}\left(x_j^b y^r dx\right) = \nu_{j,b,r+\gamma_j-b\gamma_j} x_j^b y^{r+\gamma_j-b\gamma_j} dx + \nu_{j,b-1,r+2\gamma_j-b\gamma_j} x_j^{b-1} y^{r+2\gamma_j-b\gamma_j} dx + \cdots + \nu_{j,1,r} x_j y^r dx + \sum_{k=0}^{\mu} \left(\sum_{R<r+\gamma_k-\gamma_k B} \nu_{k,B,R} x_k^B y^R dx \right) \tag{3.6}$$

where each $\nu_{k,b,r} \in k$ and $\nu_{j,b,r+\gamma_j-b\gamma_j} \neq 0$.

The elements $x_j^b y^r dx$ of A_j satisfy $0 \leq r < (p-2)/2$ for any $j \in \{0, \ldots, \mu\}$. We have already shown that if $\sigma = x_j^b y^r dx \in A$, the output of $\mathcal{C}(\sigma)$ will be contained in $Y_{j,r}$. The next lemma shows that each term of $Y_{j,r}$ is a key term of $\mathcal{C}(\omega)$ for some $\omega \in H_j$.

Lemma 6. *Suppose $0 \leq r < (p-2)/2$ and $0 \leq j \leq \mu$. Every element of $Y_{j,r}$ is a key term of $\mathcal{C}(\omega)$ for some $\omega \in H_j$.*

Proof. Let $x_j^B y^R dx \in Y_{j,r}$. Define ω to be

$$\omega = \begin{cases} x^B y^{R+\gamma_0+\gamma_0 B} dx & \text{if } j = 0, \\ x_j^B y^{R-\gamma_j+\gamma_j B} dx & \text{if } j \in \{1, \ldots, \mu\}. \end{cases}$$

Once we have shown that $\omega \in H_j$, then the key term of $\mathcal{C}(\omega)$ is $x_j^b y^r dx$.

First, consider the case when $j = 0$. We have $\omega = x^B y^{R+\gamma_0+\gamma_0 B} dx$. If $x^B y^R dx \in Y_{0,r}$ then $R \leq r - \gamma_0 - \gamma_0 B$. Notice that this means the power on y in ω is

$$R + \gamma_0 + \gamma_0 B \leq (r - \gamma_0 - \gamma_0 B) + \gamma_0 + \gamma_0 B \leq r.$$

In general, for $x^\beta y^\rho dx$ to be in H_0, we need $\rho \geq \gamma_0 + \gamma_0\beta$. For ω, this means that we need $R + \gamma_0 + \gamma_0 B \geq \gamma_0 + \gamma_0 B$ which is trivially satisfied. This, together with the power on y in ω being less than r, gives that $\omega \in H_0$.

Second, we consider the case when $j \neq 0$. We have $\omega = x_j^B y^{R-\gamma_j+\gamma_j B} dx$. If $x_j^B y^R dx \in Y_{j,r}$ then $R \leq r + \gamma_j - \gamma_j B$. Notice that this means the power on y in ω is

$$R - \gamma_j + \gamma_j B \leq (r + \gamma_j - \gamma_j B) - \gamma_j + \gamma_j B \leq r.$$

In general, for $x_j^\beta y^\rho dx$ to be in H_j, we need $\rho \geq -\gamma_j + \gamma_j\beta$. For ω, this means that we need $R - \gamma_j + \gamma_j B \geq -\gamma_j + \gamma_j B$ which is trivially satisfied. This, together with the power on y in ω being less than r, gives that $\omega \in H_j$.

□

The next lemma will show that the columns of the Cartier-Manin matrix which correspond to the elements of the sets A_ℓ do not contribute to the rank of the Cartier-Manin matrix.

Lemma 7. *Suppose $\eta \in A_k$ for some k. Then $\mathcal{C}(\eta)$ is contained in span $\{\mathcal{C}(\omega)|\omega \in \mathcal{H}\}$.*

Proof. Since $\eta \in A_k$, then $\eta = x_k^b y^r dx$ for some $0 \leq r < (p-2)/2$. Using Lemmas 4 and 5, we have that $\mathcal{C}(\eta)$ is in span$(Y_{k,r})$. By Lemma 6, $\mathcal{C}(\eta) \in$ span $\{\mathcal{C}(\omega)|\omega \in H\}$. Choose the largest ω and denote it by ω'. Choosing an appropriate coefficient, ν, there is a new expression $\mathcal{C}(\eta) - \nu\mathcal{C}(\omega')$ in which the key term of $\mathcal{C}(\omega')$ does not appear. By Lemmas 3 through 5, we know that all other terms of $\mathcal{C}(\omega')$ are key terms of $\mathcal{C}(\omega)$ for elements $\omega \in W$ which are smaller than ω'. So, every term of $\mathcal{C}(\eta) - \nu\mathcal{C}(\omega')$ is a key term of $\mathcal{C}(\omega)$ for an element of $\omega \in W$ which is smaller than ω'. Repeating this process, we can express $\mathcal{C}(\eta)$ as a linear combination $\sum_{\omega \in H} \nu_\omega \mathcal{C}(\omega)$.

□

We now know that the rank of the Cartier-Manin matrix is equal to the sum of the sizes of the sets H_ℓ, $\ell = 0, \ldots, \mu$. As $a = g -$ rank(M) and $g = |W|$, we have that $a = \sum |W_\ell| - \sum |H_\ell| = \sum_{\ell=0}^{\mu} (W_\ell - H_\ell)$. One could also compute the a-number by finding $\sum_{\ell=0}^{\mu} |A_\ell|$.

Lemma 8. *The number* $a_j = |W_j| - |H_j|$ *is*

$$\begin{cases} \frac{(p-1)d_j}{4} & \text{if } d_j \text{ even,} \\ \frac{(p-1)(d_j^2-1)}{4d_j} & \text{if } d_j \text{ odd.} \end{cases}$$

for each $j \in \{0, 1, 2, \ldots, \mu\}$.

Proof. First, consider the case when $j = 0$. The size of W_0 is given by

$$\big|W_0\big| = (p-1)(d_0-1)/2.$$

To find the size of H_0, we will count the integer points (b, r) corresponding to $x^b y^r dx \in H_0$. The lines $r = p-2-\gamma_0-\gamma_0 b$ and $r = \gamma_0 b + \gamma_0$ intersect at $b = \frac{d_0}{2} - 1 - \frac{1}{2\gamma_0}$. The largest value of b appearing in the set H_0 is

$$b' = \lfloor b \rfloor = \begin{cases} \frac{d_0-4}{2} & \text{if } d_0 \text{ is even,} \\ \frac{d_0-3}{2} & \text{if } d_0 \text{ is odd.} \end{cases}$$

Using the picture of W_0 shown earlier as a guide, we have

$$\begin{aligned} a_0 &= \big|W_0\big| - \big|H_0\big| \\ &= \frac{(p-1)(d_0-1)}{2} - \sum_{b=0}^{b'} \left[(p-2-\gamma_0-\gamma_0 b) - (\gamma_0 b + \gamma_0) + 1\right] \\ &= \frac{(p-1)(d_0-1)}{2} - \sum_{b=0}^{b'} (p-1-2\gamma_0-2\gamma_0 b) \\ &= \frac{(p-1)(d_0-1)}{2} - (p-1-2\gamma_0)\,(b'+1) + \frac{2\gamma_0\,(b')\,(b'+1)}{2} \\ &= \begin{cases} \frac{(p-1)d_0}{4} & \text{if } d_0 \text{ even,} \\ \frac{(p-1)(d_0^2-1)}{4d_0} & \text{if } d_0 \text{ odd.} \end{cases} \end{aligned}$$

Now suppose $j \neq 0$. The size of W_j is given by

$$\big|W_j\big| = (p-1)(d_j+1)/2.$$

The size of H_j will be found by counting the integer points (b, r) corresponding to $x^b y^r dx \in H_j$. The lines $r = p-2+\gamma_j-\gamma_j b$ and $r = \gamma_j b - \gamma_j$ intersect at $b = \frac{d_j}{2}+1-\frac{1}{2\gamma_j}$. The largest value of b appearing in H_j is

$$b' = \lfloor b \rfloor = \begin{cases} \frac{d_j}{2} & \text{if } d_j \text{ is even,} \\ \frac{d_j+1}{2} & \text{if } d_j \text{ is odd.} \end{cases}$$

Using the picture of W_j shown earlier as a guide, we have

$$\begin{aligned} a_j &= \left|W_j\right| - \left|H_j\right| \\ &= \frac{(p-1)(d_j+1)}{2} - \sum_{b=1}^{b'} \left[(p-2+\gamma_j-\gamma_j b) - (\gamma_j b - \gamma_j) + 1\right] \\ &= \frac{(p-1)(d_j+1)}{2} - \sum_{b=1}^{b'} (p-1+2\gamma_j - 2\gamma_j b) \\ &= \frac{(p-1)(d_j+1)}{2} - (p-1+2\gamma_j)\, b' + \frac{2\gamma_j\,(b')\,(b'+1)}{2} \\ &= \begin{cases} \frac{(p-1)d_j}{4} & \text{if } d_j \text{ even,} \\ \frac{(p-1)(d_j^2-1)}{4d_j} & \text{if } d_0 \text{ odd.} \end{cases} \end{aligned}$$

□

Lemmas 8 gives the result we were looking for.

□

Chapter 4

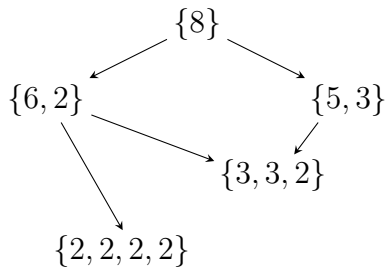
Moduli space for Artin-Schreier curves

In this chapter, we present a new result about the existence of deformations of Artin-Schreier covers with varying p-rank. This work builds on [12, 15].

4.1 Partitions

In Theorem 4.3.1, we see a connection between the p-rank of Artin-Schreier curves and a partition of the number $D+2$. First, we describe the specific partitions of $D+2$ we wish to consider. These are the partitions of $D+2$ into $r+1$ numbers $\vec{E} = \{e_1, \ldots, e_{r+1}\}$ such that each $e_j \not\equiv 1 \bmod p$. We denote the set of all such partitions by Ω_D. The subset of Ω_D which contains all partitions of length $r+1$ is denoted by $\Omega_{D,r}$. We can make a directed graph by ordering these partitions in the following way. If $\vec{E_1}$ and $\vec{E_2}$ are two partitions, we say $\vec{E_1} < \vec{E_2}$ if $\vec{E_2}$ is a refinement of $\vec{E_1}$. We draw an edge from $\vec{E_1}$ to $\vec{E_2}$ if $\vec{E_1} < \vec{E_2}$ and if there is no partition strictly between them.

As an example, let's look at the directed graph for $D = 6$ when $p = 3$:



The sets of interest are

$$\begin{aligned}
\Omega_6 &= \{\{8\},\{6,2\},\{5,3\},\{3,3,2\},\{2,2,2,2\}\} \\
\Omega_{6,0} &= \{\{8\}\} \\
\Omega_{6,1} &= \{\{6,2\},\{5,3\}\} \\
\Omega_{6,2} &= \{\{3,3,2\}\} \\
\Omega_{6,3} &= \{\{2,2,2,2\}\}.
\end{aligned}$$

Note that $\Omega_{6,r}$ is empty if $r \geq 4$.

4.2 Partitions and curves

Given a partition $\vec{E} = \{e_1, \ldots, e_{r+1}\} \in \Omega_{D,r}$, there exists an Artin-Schreier curve $y^p - y = f(x)$ where f(x) has $r+1$ poles with ramification invariants $d_j = e_j - 1$.

We look at the above example to illustrate this. The partition $\{8\}$ occurs for Artin-Schreier curves when $f(x)$ has one pole with ramification invariant 7. The partition $\{6,2\}$ occurs for Artin-Schreier curves when $f(x)$ has two poles with ramification invariants 5 and 1. The existence of such curves is given by the following lemma.

Lemma 4.2.1. *There exists an Artin-Schreier curve of p-rank $r(p-1)$ and genus g if and only if $D = \frac{2g}{p-1} \in \mathbb{Z}_{\geq 0}$ and $\Omega_{D,r} \neq \emptyset$.*

Proof. See [15, Lemma 2.7]. □

To illustrate further, we give an equation for an Artin-Schreier curve which corresponds to each partition in the example of the previous section.

Partition	Example
$\{8\}$	$y^3 - y = x^7$
$\{6, 2\}$	$y^3 - y = x^5 + \frac{1}{x}$
$\{5, 3\}$	$y^3 - y = x^4 + \frac{1}{x^2}$
$\{3, 3, 2\}$	$y^3 - y = x^2 + \frac{1}{x^2} + \frac{1}{x-1}$
$\{2, 2, 2, 2\}$	$y^3 - y = x + \frac{1}{x} + \frac{1}{x-1} + \frac{1}{x+1}$

4.3 Moduli space for Artin-Schreier curves

A moduli space for Artin-Schreier curves is an algebraic space V such that there is a bijection between maps $S \to V$ and Artin-Schreier curves defined over S. In this section, we define the two moduli spaces we will be interested in. The first is the moduli space of Artin-Schreier curves with genus g which will be denoted by AS_g. The second is the moduli space of Artin-Schreier curves with genus g and p-rank s which will be denoted by $AS_{g,s}$.

The p-rank satisfies the inequality $0 \leq s \leq g$ so we have

$$AS_g = \coprod_{s=0}^{g} AS_{g,s}.$$

The irreducible components of $AS_{g,s}$ correspond to the elements of $\Omega_{D,\frac{s}{p-1}}$ as long as $\frac{s}{p-1} \in \mathbb{Z}_{\geq 0}$. The dimensions of the irreducible components of $AS_{g,s}$ are given by the following theorem [15, Theorem 1.1].

Theorem 4.3.1. *Let $g = D(p-1)/2$ with $D \geq 1$ and $s = r(p-1)$ with $r \geq 0$.*

1. *The set of irreducible components of $AS_{g,s}$ 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 $e_j \not\equiv 1 \bmod p$.*

2. *The irreducible component of $AS_{g,s}$ for the partition $\{e_1, \ldots, e_{r+1}\}$ has dimension $D - 1 - \sum_{j=1}^{r+1} \lfloor (e_j - 1)/p \rfloor$.*

We consider the example above to illustrate. Since $p = 3$, the genus $g = D(p-1)/2 = D = 6$. We have

$$AS_6 = \coprod_{s=0}^{6} AS_{6,s}.$$

The p-rank in this case is $s = r(p-1) = 2r$. Since we only had four non-empty sets $\Omega_{6,r}$ above, we only have four moduli spaces of interest: $AS_{6,0}$, $AS_{6,2}$, $AS_{6,4}$, and $AS_{6,6}$. As a specific example, $AS_{6,2}$ has two irreducible components which correspond to the two partitions in $\Omega_{6,1}$. We denote these by $AS_{6,\{6,2\}}$ and $AS_{6,\{5,3\}}$.

In order to figure out if AS_g is connected, it is necessary to consider deformations of Artin-Schreier curves in which the p-rank varies.

4.4 Deformations

We have already seen that an Artin-Schreier curve $y^p - y = f(x)$ is a $\mathbb{Z}/p$ cover of the projective line. In this section we are interested in finding a family of covers $y^p - y = f(x,t)$ such that when $t = 0$ we have our original cover and when $t \neq 0$ we get a different cover with some desired properties. This is called a deformation. More specifically, we are interested in flat deformations. Having a flat deformation implies the genus of the curve given by $y^p - y = f(x,t)$ is constant for all values of t. Using the formula for the genus of an Artin-Schreier curve,

$$g = \left(\left(\sum_{j=1}^{r} e_j\right) - 2\right) \cdot \frac{p-1}{2},$$

we see that the genus will be constant as long as

$$\sum_{j=1}^{r} e_j = \sum_{j=1}^{r} (d_j + 1)$$

remains constant. So, the number of poles can change as long as the orders of the poles sum in the right way.

4.5 Known deformations

Let $S = \text{Spec}(k[[t]])$. The following result is presented in [15].

Proposition 4.5.1. *Suppose that $Y_\circ$ is an Artin-Schreier k-curve of genus g and p-rank $r(p-1)$. Suppose there is a ramified point of $Y_\circ$ under the $\mathbb{Z}/p$-action whose lower jump d satisfies $d \geq p+1$. Then there exists an Artin-Schreier curve Y_S over S whose special fibre is isomorphic to $Y_\circ$ and whose generic fibre has genus g and p-rank $(r+1)(p-1)$.*

This is a generalization of the deformation result which appears in [12]. Stated in the language of the previous sections, this proposition shows that an Artin-Schreier curve with partition $\vec{E_1}$ deforms to a family of Artin-Schreier curves with partition generically $\vec{E_2}$ if the edge has the form $\{e\} \to \{e_1, e_2\}$ where either e_1 or $e_2 \equiv 0 \bmod p$.

Proposition 4.5.1 shows that it is possible for the p-rank of the fibres to vary by $p-1$. In the next section, we present a situation in which the p-rank will vary by $2(p-1)$.

4.6 A new deformation

To build on the deformation result that appeared in the previous section, we consider whether an Artin-Schreier curve with a single pole can deform to a curve with three poles. This would increase the p-rank from 0 to $2(p-1)$.

Theorem 4.6.1. *Let X be an Artin-Schreier curve of genus $g = (p-1)(d-1)/2$ and p-rank 0. It is given by an affine equation $y^p - y = f(x)$ for some degree d polynomial $f(x) \in k[x]$ with $d \not\equiv 0 \bmod p$. Assume $d \geq 2p+1$ and $f(x) \in x^d k\left[x^{-p}\right]$. Then, there exists a flat deformation of X over Spec$(k[[t]])$ whose generic fibre is an Artin-Schreier curve with p-rank $2(p-1)$.*

Proof. Let b and c be such that

$$b \equiv 0 \bmod p,$$

$$c \equiv 2d \bmod p,$$

$$1 \leq c, \text{ and}$$

$$1 \leq d - b - c.$$

Note that this is possible for $d \geq 2p+1$; let $b = p$ and let $0 < c < p$ with $c \equiv 2d \bmod p$.

Let $0 < \xi < p$ be such that $\xi \equiv d \bmod p$. As $f(x) \in x^d k\left[x^{-p}\right]$, we can write $f(x) = \sum_{q=0}^{\lfloor d/p \rfloor} r_q x^{qp+\xi}$ for some coefficients $r_q \in k$. Now consider the Artin-Schreier curve $y^p - y = f(x,t)$ where

$$f(x,t) = \frac{f(x)}{(1-xt)^b(1+xt)^c}.$$

Observe that $f(x,t)$ has poles at $x = 1/t$, $x = -1/t$, and $x = \infty$. Also notice that $y^p - y = f(x,0)$ is our original curve X.

First, we will compute the ramification invariant at the pole $x = 1/t$. To do this, we will compute the Laurent expansion of $f(x,t)$ centered at $x = 1/t$. Notice that $f(x,t)$ can be rewritten as $f(x,t) = \left((-t)^{-b} f(x)/(1+xt)^c\right)(x - 1/t)^{-b}$. With this in mind, the first three coefficients of the Laurent expansion $f(x,t) = \sum_{n=-b}^{\infty} h_n(t)(x - 1/t)^n$ are

$$h_{-b}(t) = -\frac{1}{2^c t^b} \sum_{q=0}^{\lfloor d/p \rfloor} \frac{r_q}{t^{qp+\xi}},$$

$$h_{-b+1}(t) = \frac{1}{2^{c+1} t^b} \sum_{q=0}^{\lfloor d/p \rfloor} \frac{r_q\,(c - 2\xi))}{t^{qp+\xi-1}}, \text{ and}$$

$$h_{-b+2}(t) = \frac{1}{2^{c+3} t^b} \sum_{q=0}^{\lfloor d/p \rfloor} \frac{r_q\,(4c\xi - c(c+1) - 4\xi(\xi-1))}{t^{qp+\xi-2}}.$$

Since $2\xi \equiv c \bmod p$, we see that $h_{-b+1}(t) = 0$. We also notice that because $b \equiv 0 \bmod p$, we can use a change of variables to replace $h_{-b}(t)$ with its p^{th} root (Section 2.1). Our third observation is that the coefficient $h_{-b+2}(t)$ is not equal to zero because

$d \not\equiv 0 \bmod p$. Putting these three things together, the Artin-Schreier curve $y^p - y = f(x,t)$ can be written in the form $y^p - y = \tilde{f}(x,t)$ where $\tilde{f}(x,t) = \sum_{n=-b+2}^{\infty} h_n(t)(x - 1/t)^n + h_{-b}(t)^{1/p}(x-1/t)^{-b/p}$. This shows that the ramification invariant of the curve above $x = 1/t$ is $b-2$.

Computing the Laurent expansion of $f(x,t)$ centered at $x = -1/t$ shows that the ramification invariant above $x = -1/t$ is c. The last pole of $f(x,t)$ is at infinity and has ramification invariant $d - b - c$. Recall the formula for the genus of an Artin-Schreier curve from section 2.2, $g = (\sum_{j=1}^{r+1}(d_j + 1) - 2)(p-1)/2$. Using this formula, the genus of the generic fibre is

$$g = ((b-2+1) + (c+1) + (d-b-c+1) - 2)(p-1)/2) = (d-1)(p-1)/2.$$

Because the genus of the generic fibre is the same as the genus of the special fibre, the deformation is flat.

□

Appendix A

The different

Given an extension of an algebraic function field, we would like to study the relationship between the genera of the two function fields. This relationship is given by the Hurwitz genus formula. Specifically, we will try to understand the term of the Hurwitz genus formula which measures the ramification. This term is called the different. We will start by introducing some basic knowledge about algebraic function fields, valuation rings, and discrete valuations. Then we will give the necessary background for understanding the Hurwitz formula. Finally, we show some steps in the calculation of the different for a specific example. Most of the following can be found in chapters one and three of [18].

A.1 Algebraic function fields

We begin with some definitions about function fields, valuations, and valuation rings. An example using these definitions is given in the next section.

Definition A.1.1. Let K be a field. If F is a finite extension of $K(x)$ for some $x \in F$, then F/K is called an **algebraic function field**.

Definition A.1.2. The **field of constants** of F/K is the set

$$\tilde{K} = \{z \in F \mid \text{z is algebraic over } K\}.$$

K is called **algebraically closed** in F if $\tilde{K} = K$.

Definition A.1.3. A ring L is called a **valuation ring** of the function field F/K if $K \subset L \subset F$ and if $z \in F$, either $z \in L$ or $z^{-1} \in L$.

Definition A.1.4. A function $\nu : F \to \mathbb{Z} \cup \{\infty\}$ is called a **discrete valuation** of the function field F/K if it has the following properties:

1. $\nu(x) = \infty \iff x = 0$.
2. $\nu(xy) = \nu(x) + \nu(y)$ for any $x, y \in F$.
3. $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ for any $x, y \in F$.
4. There exists an element $z \in F$ with $\nu(z) = 1$.
5. $\nu(a) = 0$ for any $0 \neq a \in K$.

Here we note that the properties of a discrete valuation guarantee that it is surjective onto $\mathbb{Z} \cup \{\infty\}$.

Definition A.1.5. Suppose L is a valuation ring of F/K. Then L is a local ring. The maximal ideal P of L is called a **place** of F/K. An element $\lambda \in P$ is called a **prime element** for P if $P = \lambda L$. We also define

$$\mathbb{P}_F = \{P \mid P \text{ is a place of } F/K\}.$$

A valuation ring L of F/K is determined by its maximal ideal P :

$$L = L_P = \{z \in F \mid z^{-1} \notin P\}.$$

Definition A.1.6. Let P be a place of F/K. We can associate P with a discrete valuation $\nu_P : F \to \mathbb{Z} \cup \{\infty\}$ in the following way. If t is a prime element of P then each $x \in F$ can be written in the form $x = t^n u$ for some $n \in \mathbb{N}$ and some $u \in L^*$. Define $\nu_P(x) = n$ and $\nu_P(0) = \infty$.

Theorem A.1.7. The discrete valuation ν_P of the place P can be used to define

$$L_P = \{z \in F \mid \nu_P(z) \geq 0\},$$
$$L_P^* = \{z \in F \mid \nu_P(z) = 0\}, \text{ and}$$
$$P = \{z \in F \mid \nu_P(z) > 0\}.$$

A discrete valuation ν of F/K can be used to define a place and a valuation ring as follows:

$$P = \{z \in F \mid \nu(z) > 0\},$$
$$L_P = \{z \in F \mid \nu(z) \geq 0\}.$$

If $x \in F$, then $\nu_P(x) = 1$ if and only if x is a prime element for P.

A.2 Places and valuation rings of $K(x)$

Let K be a field and $F = K(x)$ be the field of rational functions in x. If $p(x)$ is an irreducible polynomial in $K[x]$, the corresponding valuation $\nu = \nu_{p(x)}$ measures the "divisibility by $p(x)$." In the following we let $f(x), g(x) \in K[x]$ and when we write $f(x)/g(x)$ we understand that $g(x) \neq 0$ and $\gcd(f(x), g(x)) = 1$. We have

$$\begin{aligned}
L_{p(x)} &= \{\, q(x) \in F \mid \nu(q(x)) \geq 0\} \\
&= \left\{ \frac{f(x)}{g(x)} \in F \;\middle|\; \nu(f(x)) - \nu(g(x)) \geq 0 \right\} \\
&= \left\{ \frac{f(x)}{g(x)} \in F \;\middle|\; p(x) \nmid g(x) \right\}, \\
P_{p(x)} &= \{q(x) \in F \mid \nu(q(x)) > 0\} \\
&= \left\{ \frac{f(x)}{g(x)} \in F \;\middle|\; p(x) \mid f(x), p(x) \nmid g(x) \right\}.
\end{aligned}$$

We can also define the valuation ring L_∞ and its maximal ideal P_∞ as follows:

$$L_\infty = \left\{ \frac{f(x)}{g(x)} \in F \;\middle|\; \deg(f(x)) \leq \deg(g(x)) \right\},$$
$$P_\infty = \left\{ \frac{f(x)}{g(x)} \in F \;\middle|\; \deg(f(x)) < \deg(g(x)) \right\}.$$

Notice that $\lambda = p(x)$ is a prime element for $P_{p(x)}$ and $\lambda = \frac{1}{x}$ is a prime element for P_∞.

A.3 The different

Let F/K be an algebraic function field and F'/F a finite separable extension. In this section, we define the different of an algebraic extension F'/F. This will be related to the ramification in the field extension. The different is an important part of the Hurwitz genus formula which follows in the next section.

Definition A.3.1. F'/K' is an **algebraic extension** of F/K if $F' \supseteq F$ is an algebraic field extension and $K' \supseteq K$.

We will assume F'/K' is an algebraic extension of F/K from now on.

A place $P' \in \mathbb{P}_{F'}$ of F'/K' lies over $P \in \mathbb{P}_F$ if $P' \supseteq P$. We denote this by P'/P.

Definition A.3.2. Suppose $P' \in \mathbb{P}_{F'}$ lies over $P \in \mathbb{P}_F$. The integer e for which $\nu_{P'}(x) = e \cdot \nu_P(x)$ for all $x \in F$ is called the **ramification index** and denoted by $e(P'|P)$.

If $e(P'|P) > 1$ then $P'|P$ is called **ramified** and P is called a **branch point**. If $e(P'|P) = 1$ then $P'|P$ is called **unramified**.

We now define the complementary module which will allow us to define the different exponent for each P'/P.

Definition A.3.3. Let $P \in \mathbb{P}_F$ and let L'_P be the integral closure of L_P in F'. The **complementary module** over L_P is

$$C_P = \{z \in F' \mid \mathrm{Tr}_{F'/F}(z \cdot L'_P) \subseteq L_P\}.$$

Proposition A.3.4. The complementary module has the following properties:

1. $L'_P \subseteq C_P$ and C_P is an L'_p-module.

2. There exists $t \in F'$ such that $C_P = t \cdot L'_P$.

Notice that the element t in part two of proposition A.3.4 may not be unique. However, the following definition is well defined for any choice of t which satisfies part two of the proposition.

Definition A.3.5. Let $P \in \mathbb{P}_F$ and let L'_P be the integral closure of L_P in F. Let $C_P = t \cdot L'_P$ be the complementary module over L_P. The **different exponent** of P'/P is

$$d(P'|P) = -\nu_{P'}(t).$$

Theorem A.3.6. Suppose $P' \in \mathbb{P}_{F'}$ lies over $P \in \mathbb{P}_F$. Then

1. $d(P'|P) \geq e(P'|P)$

2. $d(P'|P) = e(P'|P) - 1$ if and only if $\text{char}(K) \nmid e(P'|P)$.

We give an example of Theorem A.3.6 part 2 in section 2.5. A proof of this theorem appears in [18].

Definition A.3.7. The **different** of F'/F is the divisor

$$\text{Diff}(F'/F) = \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P) \cdot P'.$$

We can see from this definition that the different is a divisor which contains information about ramification in the function field extension. In the Hurwitz formula, we will need the degree of this divisor. First, we need to define the degree of a place.

Definition A.3.8. Let $P \in \mathbb{P}_F$. The **residue class field** of P is

$$F_P = L_P/P.$$

The **degree** of P is

$$\deg P = [F_P : K].$$

For an irreducible polynomial $p(x)$, the degree of $P_{p(x)}$ is $\deg(p(x))$.

A.4 The Hurwitz genus formula

We will use the Hurwitz formula below to compute the genus of a curve. This formula does not give much insight to the definition of the genus so we give the definition here.

Definition A.4.1. Given a smooth connected projective curve C, the **genus** of C is the dimension of the vector space of holomorphic 1-forms on C over K. More formally, the genus of C is

$$g = \dim\left(H^o\left(\Omega_1\right)\right).$$

Given an algebraic function field F/K, there exists a unique smooth projective curve C defined over K such that F is the field of rational functions on C. The genus of the function field F/K is the genus of the curve C.

We will use the following theorem to compute the genus of Artin-Schreier curves later in the paper. For a more thorough treatment of this theorem, see [18].

Theorem A.4.2 (Hurwitz Genus Formula). Let F/K and F'/K' be algebraic function fields with F'/F a finite separable extension and K' the field of constants of F'. Let g and g' denote the genus of F/K and F'/K' respectively. Then

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg \text{Diff}(F'|F).$$

A.5 Computing the different

We now show how to compute the different in a specific example. This is an example of part two of Theorem A.3.6.

Theorem A.5.1. Let K be a field of characteristic not 2. Let $F = K(x)$ and $F' = \dfrac{K(x)[y]}{y^2 - h(x)}$ where $h(x)$ has deg $h(x) = r$ distinct roots in K. Then the genus of F'/K is

$$g' = \begin{cases} \frac{r-2}{2} & \text{if } r \text{ is even,} \\ \frac{r-1}{2} & \text{if } r \text{ is odd.} \end{cases}$$

Proof. Fix the place $P = (x)$. The corresponding valuation ring is the localization $L_P = D^{-1}K[x]$ where $D = K[x] - (x)$. We have the following setup:

$$\begin{array}{lcl} F' = \frac{K(x)[y]}{(y^2 - h(x))} & \supseteq & L'_P \\ | & & \\ F = K(x) & \supseteq & L_P = D^{-1}K[x] \\ | & & \\ K & & \end{array} .$$

We now find L'_P, the integral closure of L_P in F', so we can later compute the complementary module over L_P. Since F'/F is a degree two extension, we have

$$z \in L'_P \iff \mathrm{Tr}_{F'/F}(z) \in L_P \text{ and } \mathrm{N}_{F'/F}(z) \in L_P.$$

A basis for F'/F is $\{1, y\}$ so any $z \in F'$ can be written $z = a + by$ where $a = \frac{f_1}{g_1}, b = \frac{f_2}{g_2} \in K(x)$ with each $f_i, g_i \in K[x]$. The minimal polynomial of $z = a + by \in F'$, is

$$\mathrm{min}_z(\chi) = (\chi - (a + by))(\chi - (a - by)) = \chi^2 - 2a\chi + (a^2 - b^2 h)$$

where we have used that $y^2 = h(x)$. We find $\mathrm{Tr}_{F'/F}(z) = 2a$ and $\mathrm{N}_{F'/F}(z) = a^2 - b^2 h$. We now have

$$\begin{aligned} z \in L'_P &\iff \begin{cases} 2a = 2\frac{f_1}{g_1} & \in L_P = D^{-1}K[x] \\ a^2 - b^2 h = \left(\frac{f_1}{g_1}\right)^2 - \left(\frac{f_2}{g_2}\right)^2 h & \in L_P = D^{-1}K[x] \end{cases} \\ &\iff z = \frac{f_1}{g_1} + \frac{f_2}{g_2} y, \text{ where } x \nmid g_1(x), x \nmid g_2(x) \\ &\iff z = \frac{f_1}{g_1} + \frac{f_2}{g_2} y, \text{ where } g_1(0) \neq 0, g_2(0) \neq 0. \end{aligned}$$

Now that we have L'_P, we can compute the complementary module over L_P. Using that $\{1, y\}$ is a basis for L'_P as a vector space over L_P, we can write

$$\begin{aligned} C_P &= \{z \in F' \mid \mathrm{Tr}_{F'/F}(z \cdot L'_P) \subseteq L_P\} \\ &= \{z \in F' \mid \mathrm{Tr}_{F'/F}(z \cdot \gamma) \in L_P \text{ for } \gamma \in \{1, y\}\}. \end{aligned}$$

If $z = a + by$ where a and b are defined as above, we have

$$\begin{aligned} z \in C_P &\iff \begin{cases} \mathrm{Tr}_{F'/F}(z \cdot 1) & \in L_P \\ \mathrm{Tr}_{F'/F}(z \cdot y) & \in L_P \end{cases} \\ &\iff \begin{cases} 2a & \in L_P \\ 2bh & \in L_P \end{cases} \\ &\iff \begin{cases} 2\frac{f_1}{g_1} & \in L_P \\ 2\frac{f_2}{g_2}h & \in L_P. \end{cases} \end{aligned}$$

We can see from this calculation that C_P depends on the polynomial $h(x)$. To proceed, we need to consider the two possible cases: $x \mid h(x)$ and $x \nmid h(x)$.

If $h(x)$ is not divisible by x, then the complementary module is

$$\begin{aligned} C_P &= \{\, z = a + by \mid g_1(0) \neq 0,\ g_2(0) \neq 0\} \\ &= L'_P. \end{aligned}$$

We need to write $C_P = t \cdot L'_P$ for some $t \in F'$. In this case, $t = 1$ and we have $C_P = 1 \cdot L'_P$. If P' is place lying over P, then $\nu_{P'}(t) = \nu_{P'}(1) = 0$.

Now we look at the case where x divides $h(x)$. In this case, the complementary module is given by

$$C_P = \{\, z = a + by \mid g_1(0) \neq 0,\ x^2 \nmid g_2(x)\}.$$

The difference in this case is that $g_2(x)$ is allowed to have zero as a root. We find $C_P = \frac{y}{x} \cdot L'_P$ which gives $t = y/x$ in the expression $C_P = t \cdot L'_P$. In order to compute

the different exponent, we need to find the place P' which lies over P. We find that $P' = y \cdot L'_P$ so y is a prime element for P'. The different exponent is

$$\begin{aligned} d(P'|P) &= -\nu_{P'}\left(\frac{y}{x}\right) \\ &= -\left(\nu_{P'}(y) - \nu_{P'}(x)\right) \\ &= -\left(1 - \nu_{P'}\left(y^2 \cdot \frac{x}{h(x)}\right)\right) \\ &= -(1-2) \\ &= 1. \end{aligned}$$

So $P'|P$ is ramified in the case when x divides $h(x)$.

From this calculation, we see that we will get $d(P'|P) = 1$ for each $P \in K$ corresponding to a factor of $h(x)$. In this extension, the degree of the places corresponding to the roots of $h(x)$ have degree 1. This can be seen from the $n = efr$ theorem. From the Hurwitz formula we can see that the cover will be branched at infinity if the degree of $h(x)$ is odd, and not branched over infinity if $h(x)$ has even degree. Therefore, the degree of the different for this example is

$$\text{deg Diff}\left(\frac{K(x)[y]}{(y^2 - h(x))}\middle| K(x)\right) = \begin{cases} r & \text{if } r \text{ is even,} \\ r+1 & \text{if } r \text{ is odd.} \end{cases}$$

Using this result in the Hurwitz genus formula yields the theorem. □

Appendix B

Supersingular elliptic curves

Let k be an algebraically closed field of characteristic p. An elliptic curve E defined over k can be put into its Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_i \in k$. From these coefficients, we can define

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2 \\
b_4 &= 2a_4 + a_1a_3 \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\
j &= c_4^3/\Delta
\end{aligned}$$

where Δ is the discriminant and j is the j-invariant of the elliptic curve E. Our first fact about the j-invariant is that two elliptic curves are isomorphic over $\bar{k}$ if and only if they have the same j-invariant.

Definition B.0.1. An elliptic curve E is called *supersingular* if it has no p-torsion points, that is, if $E[p](k) = \{\mathcal{O}\}$. If $E[p](k) \neq \{\mathcal{O}\}$, E is called *ordinary.*

Example B.0.2. The only supersingular elliptic curve over a field of characteristic $p = 2$ is the curve with j-invariant 0. We need to show that an elliptic curve with no 2-torsion points has j-invariant 0. Let $P = (x, y) \in E$, then the multiplication by 2 map has x-coordinate $\frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}$. In characteristic 2, this can be simplified to $\frac{x^4 - b_4x^2 - b_8}{b_2x^2 + b_6}$. In order for there to be no 2-torsion points, $b_2x^2 + b_6 \neq 0$ which implies

$$\begin{aligned} 0 &\neq b_2x^2 + b_6 \\ 0 &\neq (a_1^2)x^2 + (a_3^2) \\ 0 &\neq (a_1x + a_3)^2 \\ a_1 &= 0 \text{ and } a_3 \neq 0. \end{aligned}$$

With $a_1 = 0$ and $a_3 \neq 0$, the discriminant is

$$\begin{aligned} \Delta &= b_2^2b_8 + b_6^2 + b_2b_4b_6 \\ &= (a_1^2)^2(a_1^2a_6 + a_1a_3a_4) + (a_3^2)^2 + (a_1^2)(a_1a_3)(a_3^2) \\ &= a_3^4 \\ &\neq 0. \end{aligned}$$

Using that $a_1 = 0$ and $\Delta \neq 0$, we see the j-invariant is

$$j = \frac{c_4^3}{\Delta} = \frac{b_2^2}{\Delta} = \frac{(a_1^2)^2}{\Delta} = 0.$$

Proposition B.0.3. If E is defined over a field k with $\mathrm{char(k)} \neq 2$, then
(a) E is isomorphic to some $E_\lambda : y^2 = x(x-1)(x-\lambda)$ where $\lambda \in \bar{k}$ and $\lambda \neq 0, 1$.
(b) The j-invariant of E_λ is $j(E_\lambda) = \frac{2^8(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$.
(c) The map from $\bar{k}\backslash\{0, 1\} \to \bar{k}$ defined by $\lambda \mapsto j(E_\lambda)$ is two-to-one over $j = 0$, three-to-one over $j = 1728$, and six-to-one over all other j.

Theorem B.0.4. Let E be an elliptic curve defined over a finite field k with characteristic $p > 2$.

(a) Suppose $E : y^2 = f(x)$ where $f(x)$ is a degree three polynomial with distinct roots in $\bar{k}$. Then E is supersingular if and only if the x^{p-1} coefficient of $f(x)^{(p-1)/2}$ is zero.

(b) Define the polynomial $H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i$ where $m = (p-1)/2$. Then $H_p(\lambda) = 0$ if and only if $E_\lambda : y^2 = x(x-1)(x-\lambda)$ is supersingular.

(c) The number of supersingular elliptic curves, up to isomorphism, in characteristic p is $\lfloor p/12 \rfloor + \epsilon_p$ where

$$\epsilon_3 = 1$$

$$\epsilon_p = 0 \text{ if } p \equiv 1 \bmod 12$$

$$\epsilon_p = 1 \text{ if } p \equiv 5, 7 \bmod 12$$

$$\epsilon_p = 2 \text{ if } p \equiv 11 \bmod 12.$$

This theorem is stated in [17]. The following examples illustrate part (c) of Theorem B.0.4.

Example B.0.5. Let $p = 3$, then $m = \frac{p-1}{2} = 1$. From part (b) of the theorem, $H_p(t) = \sum_{i=0}^{1} \binom{1}{i}^2 t^i = 1 + t$. The only root of this polynomial is $t = -1$ which gives the elliptic curve $E_{-1} : y^2 = x(x-1)(x+1)$.

Example B.0.6. Let $p \geq 5$ and let $E : y^2 = x^3 + 1$ be the elliptic curve with j-invariant zero. For which primes is this elliptic curve supersingular? Part (a) of the theorem above tells us that we need to look at the coefficient of x^{p-1} in $(x^3+1)^{(p-1)/2}$. The x^{p-1} term of this polynomial only appears if $3|(p-1)$. In this case, the coefficient is $\binom{(p-1)/2}{(p-1)/3}$. Thus, E is ordinary if $p \equiv 1 \bmod 3$, and supersingular if $p \equiv 2 \bmod 3$.

Example B.0.7. If $p \geq 3$, the elliptic curve $E : y^2 = x^3 + x$ with j-invariant 1728 is ordinary if $p \equiv 1 \bmod 4$ and supersingular if $p \equiv 3 \bmod 4$.

Appendix C

Maple code for computing the a-number

```
randomize():

with(linalg):
with(ArrayTools):

#pick a prime and degree for the pole at infinity
p:=7:
d[0]:=3:

#number of extra poles and degrees of the poles
numpoles:=1:
d[1]:=3:
#d[2]:=2:
#d[3]:=3:
#locations of the poles (does not support x=0 as a pole location)
e[1]:=1:
#e[2]:=2:
```

```
#e[3]:=3:

#Gammas
for i from 0 to numpoles do
    gam[i]:=(p-1)/d[i]:
end do:

#compute the genus
genussum:=0:
for i from 0 to numpoles do
    genussum:=genussum + (d[i]+1):
end do:
genus:=(genussum-2)*(p-1)/2:

#compute expected a-number
expectedanum:=0:
for i from 0 to numpoles do
    if type(d[i],even) then
        anumpart[i]:=(p-1)*d[i]/4:
    else
        anumpart[i]:=(p-1)*(d[i]^2-1)/(4*d[i]):
    end if:
    expectedanum:=expectedanum + anumpart[i]:
end do:

#compute the basis of 1-forms for both the input and output
n:=0:
m:=0:
maxbound:=0:
A:=Array(1..genus,1..3):
```

```
A2:=Array(1..genus,1..3):

for i from 0 to numpoles do
  if i=0 then
      bound[i]:=(p-1)*(d[i]-1)-2:
  else
      bound[i]:=(p-1)*(d[i]+1):
  end if:
  maxbound:=max(maxbound,bound[i]):
end do:

#Basis built left to right
for r from 0 to maxbound do
  for b from 0 to bound[0] do
    if (r*d[0]+b*p <= bound[0]) then
        n:=n+1;
        A[n,1]:=b;
        A[n,2]:=r;
        A[n,3]:=0:
    end if:
  end do:
  for i from 1 to numpoles do
    for b from 0 to bound[i] do
      if b>0 and (r*d[i]+b*p <= bound[i]) then
          n:=n+1;
          A[n,1]:=-b;
          A[n,2]:=r;
          A[n,3]:=e[i]:
      end if:
    end do:
```

```
  end do:
end do:

#Use same output basis
A2:=A;

#Build function to test
 r1:=rand(0..(p-1)):
 r2:=rand(1..(p-1)):

 func:=x^(d[0]):

 for i from (d[0]-1) to 0 by -1 do
   if i mod p <>0 then
     a:=r1():
     func:=func + a*x^i:
   end if:
   if i=0 then
     a:=r1():
     func:=func + a:
   end if:
 end do:

 for j from 1 to numpoles do
   for i from -1 to -(d[j]-1) by -1 do
     if i mod p <>0 then
       a:=r1():
       func:=func + a*(x+e[j])^i:
     end if:
   end do:
```

```
end do:

m:=1:

for j from 1 to numpoles do
    a:=r2():
    func:=func + a/(x+e[j])^d[j]:
end do:

#Build Cartier Matrix
C:=Array(1..genus,1..genus):

for k from 1 to genus do

  g:=A[k];

  if g[2]<>0 then
    if g[3]=0 then
        h:=x^g[1]*(y^p - func)^g[2];
        h:=sort(expand(convert(h,parfrac,x)),x) mod p;
        H:=nops(h):
    end if:
    for i from 1 to numpoles do
      if g[3]=e[i] then
        h:=(y^p - func)^g[2]*(x+e[i])^g[1];
        h:=sort(expand(convert(h,parfrac,x)),x) mod p;
        H:=nops(h):
      end if:
    end do:
  else
```

```
    if g[3]=0 then
        h:=x^g[1];
        H:=1:
    end if:
    for i from 1 to numpoles do
      if g[3]=e[i] then
        h:=(x+e[i])^g[1];
        H:=1:
      end if:
    end do:
  end if:

  j:=Array(1..H,1..4):

  h2:=0:
  if H=1 then
      if degree(h,x) mod p=(p-1) then
          temp:=h:
          h2:=h2+x^(floor(degree(temp,\
x)/p))*y^(degree(temp,y)/p)*temp/(x^degree(temp,x)*y^degree(temp,y)):
          j(1,1):=floor(degree(temp,x)/p):
          j(1,2):=degree(temp,y)/p:
          j(1,3):=0:
          j(1,4):=simplify(temp/(x^degree(temp,x)*y^degree(temp,y))) mod p:
      end if:
      for n from 1 to numpoles do
        if degree(h,x+e[n]) mod p=(p-1) then
          temp:=h:
          h2:=h2+temp*(x+e[n])^(-degre\
e(temp,x+e[n]))/y^degree(temp,y)*y^(de\
```

```
gree(temp,y)/p)/(x+e[n])^ceil((-degree(temp,x+e[n]))/p):
          j(1,1):=-ceil((-degree(temp,x+e[n]))/p):
          j(1,2):=degree(temp,y)/p:
          j(1,3):=e[n]:
          j(1,4):=simplify(temp*(x+e[n\
])^(-degree(temp,x+e[n]))/y^degree(temp,y)) mod p:
        end if:
      end do:
  else
    for i from 1 to H do
      if degree(op(i,h),x) mod p=(p-1) then
          temp:=op(i,h):
          h2:=h2+x^(floor(degree(temp,\
x)/p))*y^(degree(temp,y)/p)*temp/(x^degree(temp,x)*y^degree(temp,y)):
          j(i,1):=floor(degree(temp,x)/p):
          j(i,2):=degree(temp,y)/p:
          j(i,3):=0:
          j(i,4):=simplify(temp/(x^degree(temp,x)*y^degree(temp,y))):
      end if:
      for n from 1 to numpoles do
        if degree(op(i,h),x+e[n]) mod p=(p-1) then
          temp:=op(i,h):
          h2:=h2+temp*(x+e[n])^(-degre\
e(temp,x+e[n]))/y^degree(temp,y)*y^(de\
gree(temp,y)/p)/(x+e[n])^ceil((-degree(temp,x+e[n]))/p):
          j(i,1):=-ceil((-degree(temp,x+e[n]))/p):
          j(i,2):=degree(temp,y)/p:
          j(i,3):=e[n]:
          j(i,4):=simplify(temp*(x+e[n\
])^(-degree(temp,x+e[n]))/y^degree(temp,y)):
```

```
          end if:
        end do:
      end do:
    end if:

    for i from 1 to H do
        nope:=0:
        if j[i,4] <> 0 then
          for q from 1 to genus do
            if IsEqual(j(i,1..3),A2(q,1..3)) then
              C[q,k]:=C[q,k]+j[i,4];
              nope:=1:
              break;
            end if:
          end do:
          if nope=0 then
              print(i):
              break:
          end if:
        end if:
      end do:

 end do:

#Compute the rank of the Cartier matrix.
C:=Matrix(C):
#Compute the a-number
anum:=genus-rank(C):

print(p):
```

```
print(func):

print(anum,expectedanum):
```

Bibliography

[1] R. Blache, *First vertices for generic Newton polygons, and p-cyclic coverings of the projective line*, arXiv: 0912.2051v1.

[2] R. Blache, *p-Density, exponential sums and Artin-Schreier curves*, arXiv: 0812.3382v1.

[3] R. Blache, É. Férard, and H. J. Zhu, *Hodge-Stickelberger polygons for L-functions of exponential sums of $P(x^s)$*, Mathematical research letters 15.5 (2008): 1053-1071.

[4] T. Ekedahl, *On Supersingular curves and Abelian Varieties*, Mathematica Scandinavica, Vol. 60 pg. 151-178.

[5] A. Elkin, *The Rank of the Cartier Operator on Cyclic Covers of the Projective Line*, arXiv:mathAG/0708.0431v1.

[6] A. Garcia and H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Inventiones mathematicae 121.1 (1995): 211-222.

[7] D. Glass, *The 2-ranks of hyperelliptic curves with extra automorphisms*, International journal of number theory 5.5 (2009): 897-910.

[8] E. Z. Goren, *Lectures on Hilbert modular varieties and modular forms. With the assistance of Marc-Hubert Nicole*, CRM Monograph Series, 14. American Mathematical Society, Providence, RI, 2002.

[9] J.W.P. Hirschfeld, G. Korchmaros, and F. Torres, *Algebraic Curves over a Finite Field*, Princeton University Press, 2008.

[10] A. Lauder and D. Wan, *Computing zeta functions of Artin-Schreier curves over finite fields*, LMS journal of computation and mathematics 5 (2002): 34-55.

[11] A. Lauder and D. Wan, *Computing zeta functions of Artin-Schreier curves over finite fields II*, Journal of complexity 20.2-3 (2004): 331-349.

[12] A. Mézard, *Quelques problémes de déformations en caractéristique mixte*, thése de doctorat de mathématiques de l'université Joseph Fourier.

[13] E. Nart and D. Sadornil, *Hyperelliptic curves of genus three over finite fields of even characteristic*, Finite fields and their applications 10.2 (2004): 198-220.

[14] R. Pries, *Jacobians of Quotients of Artin-Schreier curves*, Recent Progress in Arithmetic and Algebraic Geometry, CONM. 386 (2005) pg. 145-156.

[15] R. Pries and H. J. Zhu, *The p-rank stratification of Artin-Schreier curves*, arXiv:math.NT/0609657v2.

[16] J. Scholten and H. J. Zhu, *Slope estimates of Artin-Schreier curves*, Compositio Mathematica 137.3 (2003): 275-292.

[17] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1986.

[18] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, 1993.

[19] F. Sullivan, *p-torsion in the class group of curves with too many automorphisms*, Archiv der Mathematik 26 (1975): 253-261.

[20] G. van der Geer and M. van der Vlugt, *Artin-Schreier curves and codes*, Journal of algebra 139.1 (1991): 256-272.

[21] G. van der Geer and M. van der Vlugt, *An asymptotically good tower of curves over the field with eight elements*, The bulletin of the London Mathematical Society 34.3 (2002): 291-300.

[22] G. van der Geer and M. van der Vlugt, *Fibre products of Artin-Schreier curves and generalized Hamming weights of codes*, Journal of combinatorial theory. Series A 70.2 (1995): 337-348.

[23] N. Yui, *On the Jacobian Varieties of Hyperelliptic Curves over Fields of Characteristic* $p > 2$, J. Algebra 52 (1978), 378-410.