Families of Artin-Schreier curves with Cartier-Manin matrix of constant rank

Shawn Farnell and Rachel Pries

March 13, 2013

Abstract

Let k be an algebraically closed field of characteristic $p > 0$. Every Artin-Schreier k-curve X has an equation of the form $y^p - y = f(x)$ for some $f(x) \in k(x)$ such that p does not divide the least common multiple L of the orders of the poles of $f(x)$. Under the condition that $p \equiv 1 \bmod L$, Zhu proved that the Newton polygon of the L-function of X is determined by the Hodge polygon of $f(x)$. In particular, the Newton polygon depends only on the orders of the poles of $f(x)$ and not on the location of the poles or otherwise on the coefficients of $f(x)$. In this paper, we prove an analogous result about the a-number of the p-torsion group scheme of the Jacobian of X, providing the first non-trivial examples of families of Jacobians with constant a-number. Equivalently, we consider the semi-linear Cartier operator on the sheaf of regular 1-forms of X and provide the first non-trivial examples of families of curves whose Cartier-Manin matrix has constant rank.

Keywords: Cartier operator, Cartier-Manin matrix, Artin-Schreier curve, Jacobian, a-number.
MSC: 15A04, 15B33, 11G20, 14H40.

1 Introduction

Suppose k is an algebraically closed field of characteristic $p > 0$ and X is an Artin-Schreier k-curve, namely a smooth projective connected k-curve which is a $\mathbb{Z}/p$-Galois cover of the projective line. Studying the p-power torsion of the Jacobian of X is simultaneously feasible and challenging. For example, zeta functions of Artin-Schreier curves over finite fields are analyzed in [12, 13, 15, 19]. Newton polygons of Artin-Schreier curves are the focus of the papers [1, 2, 3, 20, 24].

Every Artin-Schreier k-curve X has an equation of the form $y^p - y = f(x)$ for some non-constant rational function $f(x) \in k(x)$ such that p does not divide the order of any of the poles of $f(x)$. The genus of X depends only on the orders of the poles of $f(x)$. Let $m + 1$ denote the number of poles of $f(x)$ and let $d_0, \ldots, d_m$ denote the orders of the poles. By the Riemann-Hurwitz formula, the genus of X is $g_X = D(p-1)/2$ where $D = \sum_{j=0}^{m}(d_j + 1) - 2$. By definition, the p-rank of the Jacobian $\mathrm{Jac}(X)$ of X is the dimension s_X of $\mathrm{Hom}(\mu_p, \mathrm{Jac}(X)[p])$ as a vector space over $\mathbb{F}_p$ where μ_p denotes the kernel of Frobenius morphism F on the multiplicative group scheme $\mathbb{G}_m$. The p-rank also equals the length of the slope 0 portion of the Newton polygon of the L-polynomial of X; (see Remark 3.1 for the definition of the Newton polygon). For an Artin-Schreier curve X, the p-rank s_X equals $m(p-1)$ by the Deuring-Shafarevich formula, and thus depends only on the number of poles of $f(x)$.

In most cases, the Newton polygon of X is not determined by the orders of the poles of $f(x)$. One exception was found by Zhu: let L denote the least common multiple of the orders of the poles of $f(x)$; under the condition that $p \equiv 1 \bmod L$, the Newton polygon of X, shrunk by the factor $p-1$ in the horizontal and vertical direction, equals the Hodge polygon of $f(x)$ [26, Corollary

1.3]; (see Remark 3.1 for the definition of the Hodge polygon). In particular, this means that the Newton polygon depends only on the orders of the poles of $f(x)$ and not on the location of the poles or otherwise on the coefficients of $f(x)$. In this paper, we prove an analogous result about the a-number of the Jacobian $\mathrm{Jac}(X)$ or, equivalently, about the rank of the Cartier-Manin matrix of X.

The a-number is an invariant of the p-torsion group scheme $\mathrm{Jac}(X)[p]$. Specifically, if α_p denotes the kernel of Frobenius on the additive group $\mathbb{G}_a$, then the a-number of (the Jacobian of) X is $a_X = \dim_k \mathrm{Hom}(\alpha_p, \mathrm{Jac}(X)[p])$. It equals the dimension of the intersection of $\mathrm{Ker}(F)$ and $\mathrm{Ker}(V)$ on the Dieudonné module of $\mathrm{Jac}(X)[p]$, where V is the Verschiebung morphism. The a-number and the Newton polygon place constraints upon each other, but do not determine each other, see e.g., [10, 11].

The a-number is the co-rank of the Cartier-Manin matrix, which is the matrix for the modified Cartier operator on the sheaf of regular 1-forms of X. The modified Cartier operator is the $1/p$-linear map $\mathcal{C} : H^0(X, \Omega^1_X) \to H^0(X, \Omega^1_X)$ taking exact 1-forms to zero and satisfying $\mathcal{C}(f^{p-1}df) = df$. In other words, the a-number equals the dimension of the kernel of $\mathcal{C}$ on $H^0(X, \Omega^1_X)$.

In this paper, under the condition $p \equiv 1 \bmod L$, we prove that the a-number of X depends only on the orders of poles of $f(x)$ and not on the location of the poles or otherwise on the coefficients of $f(x)$ (see section 3.6).

Theorem 1.1. *Let X be an Artin-Schreier curve with equation $y^p - y = f(x)$, with $f(x) \in k(x)$. Suppose $f(x)$ has $m+1$ poles, with orders $d_0, \ldots, d_m$, and let $L = \mathrm{LCM}(d_0, \ldots, d_m)$. If $p \equiv 1 \bmod L$, then the a-number of X is*

$$a_X = \sum_{j=0}^{m} a_j, \quad \textit{where} \quad a_j = \begin{cases} (p-1)d_j/4 & \textit{if } d_j \textit{ even,} \\ (p-1)(d_j-1)(d_j+1)/(4d_j) & \textit{if } d_j \textit{ odd.} \end{cases}$$

To our knowledge, Theorem 1.1 provides the first non-trivial examples of families of Jacobians with constant a-number when $p \geq 3$. When $p = 2$, the main result of [8] is that the Ekedahl-Oort type (and a-number) of an Artin-Schreier curve depend only on the orders of the poles of $f(x)$. For arbitrary p, it is easy to construct families of Jacobians with $a_X = 0$ (ordinary) or $a_X = 1$ (almost ordinary) and a family of Jacobians with $a_X = 2$ is constructed in [9, Corollary 4].

For fixed p, the families in Theorem 1.1 occur for every genus g which is a multiple of $(p-1)/2$. The a-number of each curve in the family is roughly half of the genus. Using [17, Theorem 1.1 (2)], the dimension of the family can be computed to be $\sum_{i=0}^{m}(d_j + 1) - 3 = 2g/(p-1) - 1$.

Other results about a-numbers of curves can be found in [6, 7]. We end the paper with some open questions motivated from this work.

The second author was partially supported by NSF grant DMS-1101712.

2 Background

2.1 Artin-Schreier curves

Let k be an algebraically closed field of characteristic $p > 0$. A *curve* in this paper is a smooth projective connected k-curve. An *Artin-Schreier curve* is a curve X which admits a $\mathbb{Z}/p$-Galois cover of the projective line. Letting x be a coordinate on the projective line, every Artin-Schreier curve has an equation of the form $y^p - y = f(x)$ for some non-constant rational function $f(x) \in k(x)$. By Artin-Schreier theory, after a change of variables, $f(x)$ can be chosen such that p does not divide the order of any pole of $f(x)$. We assume that this is the case throughout the paper.

Let $\mathbb{B} \subset \mathbb{P}^1(k)$ be the set of poles of $f(x)$ and suppose $\#\mathbb{B} = m+1$. We can assume that $\infty \in \mathbb{B}$ after a fractional linear transformation. We choose an ordering of the poles $\mathbb{B} = \{b_0, \ldots, b_m\}$ such that $b_0 = \infty$. For $b_j \in \mathbb{B}$, let d_j be the order of the pole of $f(x)$ at b_j. Let $x - e_j$ be a uniformizer at b_j for $1 \leq j \leq m$. Let $x_0 = x$ and let $x_j = (x - e_j)^{-1}$ if $1 \leq j \leq m$. The partial fraction decomposition of $f(x)$ has the form:

$$f(x) = f_0(x) + \sum_{j=1}^{m} f_j\left(\frac{1}{x - e_j}\right) = \sum_{j=0}^{m} f_j\left(x_j\right),$$

where $f_j(x_j) \in k[x_j]$ is a polynomial of degree d_j for $0 \leq j \leq m$ and $f_j(x)$ has no constant term for $1 \leq j \leq m$. Let $u_j \in k^\times$ be the leading coefficient of $f_j(x_j)$.

2.2 The genus and p-rank of an Artin-Schreier curve

The genus of a curve X is the dimension of the vector space $H^0(X, \Omega^1_X)$ of regular 1-forms. By the Riemann-Hurwitz formula [21, Proposition VI.4.1], the genus of an Artin-Schreier curve $X : y^p - y = f(x)$ where $f(x)$ has $m+1$ poles with prime-to-p orders $d_0, \ldots, d_j$ as described in Section 2.1 is

$$g_X = D(p-1)/2 \text{ where } D = -2 + \sum_{j=0}^{m}(d_j + 1).$$

Given a smooth projective k-curve X of genus g, let $\mathrm{Jac}(X)[p]$ denote the p-torsion group scheme of the Jacobian of X. Let μ_p be the kernel of Frobenius on the multiplicative group $\mathbb{G}_m$. The *p-rank* of X is $s_X = \dim_{\mathbb{F}_p}\mathrm{Hom}(\mu_p, \mathrm{Jac}(X)[p])$. The number of p-torsion points of $\mathrm{Jac}(X)(k)$ satisfies $\#\mathrm{Jac}(X)\,[p]\,(k) = p^{s_X}$. The p-rank of a curve satisfies the inequality $0 \leq s_X \leq g$. By a special case of the Deuring-Shafarevich formula, see [22, Theorem 4.2] or [5], if X is an Artin-Schreier curve with equation $y^p - y = f(x)$ as described above, then the p-rank of X is $s_X = m(p-1)$.

2.3 The a-number

Let α_p be the kernel of Frobenius on the additive group $\mathbb{G}_a$. The *a-number* of X is $a_X = \dim_k \mathrm{Hom}(\alpha_p, \mathrm{Jac}(X)[p])$. Equivalently, the a-number is the dimension of $\mathrm{Ker}(F) \cap \mathrm{Ker}(V)$ on the Dieudonné module of $\mathrm{Jac}(X)[p]$. The a-number also equals the dimension of $\mathrm{Ker}(V)$ on $H^0(X, \Omega^1_X)$ [14, Equation 5.2.8]. One sees that $0 \leq a_X + s_X \leq g$.

The a-number is an invariant of the p-torsion group scheme $\mathrm{Jac}(X)[p]$. In some cases, it gives information about the decomposition of the abelian variety $\mathrm{Jac}(X)$. If $a_X = g$, then $\mathrm{Jac}(X)$ is isomorphic to a product of supersingular elliptic curves [16]. If $s_X < g$, then $a_X > 0$, because there is a non-trivial local-local summand of $\mathrm{Jac}(X)[p]$ on which V is nilpotent. This can be used to show that the number of factors appearing in the decomposition of $\mathrm{Jac}(X)$ into simple principally polarized abelian varieties is at most $s_X + a_X$.

Remark 2.1. In [18], formulas are given for the a-number of an Artin-Schreier curve when $f(x)$ is a monomial x^d with $p \nmid d$. If $p \equiv 1 \bmod d$, then the main result of this paper extends [18, Corollary 3.3] to all Artin-Schreier curves $X : y^p - y = f(x)$ having the property that the orders of the poles of $f(x)$ divide $p-1$. If $p \not\equiv 1 \bmod d$, let $h_b \in [0, p-1]$ be the integer such that $h_b \equiv (-1-b)d^{-1} \bmod p$. By [18, Remark 3.4], the a-number of $X : y^p - y = x^d$ is given by

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

2.4 The Cartier operator and the a-number

The "modified" Cartier operator $\mathcal{C}$ is the semi-linear map $\mathcal{C} : H^0(X, \Omega^1_X) \to H^0(X, \Omega^1_X)$ with the following properties: $\mathcal{C}(\omega_1 + \omega_2) = \mathcal{C}(\omega_1) + \mathcal{C}(\omega_2)$; $\mathcal{C}(f^p\omega) = f\mathcal{C}(\omega)$; and

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

Suppose $\beta = \{\omega_1, \ldots, \omega_g\}$ is a basis for $H^0(X, \Omega^1_X)$. For each ω_j, let $m_{i,j} \in k$ be such that

$$\mathcal{C}\left(\omega_j\right) = \sum_{i=1}^{g} m_{i,j}\, \omega_i.$$

The $g \times g$-matrix $M = (m_{i,j})$ is the (modified) Cartier-Manin matrix and it gives the action of the (modified) Cartier operator. The Cartier-Manin matrix is $\widetilde{M} = (m^p_{i,j})$; it is the matrix for the (unmodified) Cartier operator, see [25]. The action of V is the same as the action of the (unmodified) Cartier operator on $H^0(X, \Omega^1)$, see [4], and so the a-number satisfies $a_X = g_X - \text{rank}(\widetilde{M}) = g_X - \text{rank}(M)$. At the risk of confusion, we drop the word modified in the rest of the paper.

3 The a-number of a family of Artin-Schreier curves

3.1 Regular 1-forms on an Artin-Schreier curve

Let X be an Artin-Schreier curve as described in Section 2.1. By [23, Lemma 1], a basis for $H^0(X, \Omega^1_X)$ is given by $W = \cup_{j=0}^{r} W_j$ where

$$W_0 = \left\{x^b y^r dx \mid r, b \ge 0 \text{ and } rd_0 + bp \le (p-1)(d_0 - 1) - 2\right\}, \text{ and}$$
$$W_j = \left\{x_j^b y^r dx \mid r \ge 0, b \ge 1, \text{ and } rd_j + bp \le (p-1)(d_j + 1)\right\} \text{ if } 1 \le j \le m.$$

There is a slight difference between the cases $j = 0$ and $1 \le j \le m$. This is in some way unavoidable as can be seen from the formula for the p-rank. To shorten the exposition, we let $\epsilon_j = -1$ if $j = 0$ and $\epsilon_j = 1$ if $1 \le j \le m$. Note that $\#W_j = (d_j + \epsilon_j)(p-1)/2$.

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

3.2 Action of the Cartier operator

Consider the action of the Cartier operator on $H^0(X, \Omega^1_X)$. In general,

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

To simplify notation, let $\tau = (\tau_{-1}, \ldots, \tau_m)$ denote a tuple of length $m + 2$ whose entries are non-negative integers and let $|\tau| = \sum_{j=-1}^{m} \tau_j$. Using the extended binomial theorem, we see that

$$\left(y^p - f(x)\right)^r = \sum_{\tau, |\tau| = r} c_\tau y^{p\tau_{-1}} f_0^{\tau_0}(x) f_1^{\tau_1}\left(x_1\right) \cdots f_m^{\tau_m}\left(x_m\right),$$

where

$$c_\tau = (-1)^{r-\tau_{-1}} \binom{r}{\tau_{-1}, \dots, \tau_m}.$$

So,

$$\mathcal{C}\left(x_j^b y^r\,dx\right) = \sum_{\tau, |\tau|=r} c_\tau y^{\tau-1} \mathcal{C}\left(x_j^b f_0^{\tau_0}(x) f_1^{\tau_1}(x_1) \cdots f_m^{\tau_m}(x_m)\,dx\right). \tag{1}$$

One can check that

$$\mathcal{C}\left(x_j^{ap+\epsilon_j}\,dx\right) = x_j^{a+\epsilon_j}\,dx. \tag{2}$$

3.3 An assumption on the orders of the poles

Let $L = \mathrm{LCM}(d_0, \dots, d_m)$. From now on, we assume that $p \equiv 1 \bmod L$; in other words, the order d_j of the jth pole of $f(x)$ divides $p-1$ and we define $\gamma_j = (p-1)/d_j$ for $0 \le j \le m$. Under this condition, we prove a result about the a-number of the Jacobian of X which is analogous to the following result of Zhu:

Remark 3.1. Suppose $f(x) \in \mathbb{F}_q(x)$ with $q = p^a$ and let $N_s = \#X(\mathbb{F}_{q^s})$ for $s \in \mathbb{N}$. Since X is a smooth projective curve, the zeta function of X is a rational function of the form:

$$Z_X(u) := \exp\left(\sum_{s=1}^{\infty} \frac{N_s u^s}{s}\right) = \frac{L_X(u)}{(1-u)(1-qu)},$$

where the L-function $L_X(u) \in \mathbb{Z}[u]$ is a polynomial of degree $2g$. Let v_i be the p-adic valuation of the coefficient of T^i in $L_X(u)$ for $0 \le i \le 2g$. The Newton polygon of X is the lower convex hull of $(i, v_i/a)$.

Recall that the function $f(x)$ has $m+1$ poles of orders $d_0, \dots, d_m$. Consider the multi-set of rational numbers $\Lambda = \cup_{i=0}^m \{1/d_j, \dots, (d_j-1)/d_j\}$. The Hodge polygon of $f(x)$ is the lower convex polygon in $\mathbb{R}^2$, with initial point $(0,0)$, constructed with a line segment with slope 0 with horizontal length m, then line segments with the slopes $\lambda \in \Lambda$ in increasing order with horizontal length 1 and then a line segment of slope 1 with horizontal length m.

Under the condition $p \equiv 1 \bmod L$, Zhu proved that the Newton polygon of $L_X(u)$ (shrunk by a factor of $p-1$ in the horizontal and vertical direction) equals the Hodge polygon of $f(x)$ [26, Corollary 1.3]. In particular, this means that the Newton polygon depends only on the orders of the poles of $f(x)$ and not on the location of the poles or otherwise on the coefficients of $f(x)$.

Under the condition $p \equiv 1 \bmod L$, for $0 \le j \le m$, the 1-forms $x_j^b y^r dx \in W_j$ are in bijection with ordered pairs (b, r) of integers in the closed triangle bounded by $r = 0$, $b = (1+\epsilon_j)/2$, and $r = (p - 2 + \epsilon_j \gamma_j) - \gamma_j b$.

3.4 Linearly independent columns of the Cartier-Manin matrix

In this section, we define a subset $H \subset W$ and show that the columns of the Cartier-Manin matrix associated with elements of H are linearly independent. This gives a lower bound on the rank of the Cartier-Manin matrix, and thus an upper bound on the a-number.

Recall that $\epsilon_j = -1$ if $j = 0$ and $\epsilon_j = 1$ if $1 \le j \le m$. We partition the 1-forms in W_j into two subsets:

$$H_j = \left\{ x_j^b y^r dx \in W_j \mid r \ge (b - \epsilon_j)\gamma_j \right\},$$

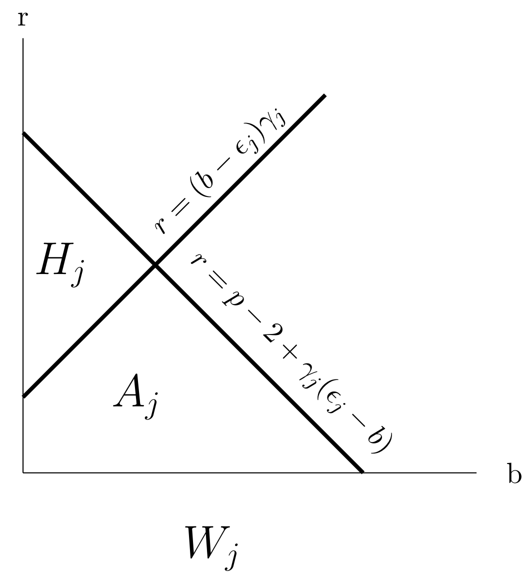

Figure 1: The subsets H_j and A_j of W_j.

and the set-theoretic complement

$$A_j = W_j - H_j.$$

Let $H = \cup_{j=0}^{m} H_j$ and $A = \cup_{j=0}^{m} A_j$.

Definition 3.2. If $\omega = x_j^b y^r dx \in H_j$, the *key term* $\kappa(\mathcal{C}(\omega))$ of $\mathcal{C}(\omega)$ is the 1-form $x_j^b y^{r-(b-\epsilon_j)\gamma_j} dx$.

Lemma 3.3. *If $\omega \in H$, the coefficient of $\kappa(\mathcal{C}(\omega))$ is non-zero in $\mathcal{C}(\omega)$.*

Proof. Suppose $\omega \in H_j$ for some $0 \leq j \leq m$. The claim is that, if $r \geq (b - \epsilon_j)\gamma_j$, then the coefficient of the 1-form $x_j^b y^{r-(b-\epsilon_j)\gamma_j} dx$ in $\mathcal{C}(x_j^b y^r dx)$ is non-zero. Consider the tuple τ given by $\tau_{-1} = r - (b - \epsilon_j)\gamma_j$, $\tau_j = (b - \epsilon_j)\gamma_j$, and $\tau_i = 0$ for all $i \notin \{-1, j\}$. If $r \geq (b - \epsilon_j)\gamma_j$, by Equation (1), the following term appears in $\mathcal{C}(x_j^b y^r dx)$:

$$c_\tau y^{r-(b-\epsilon_j)\gamma_j} \mathcal{C}\left(x_j^b f_j^{(b-\epsilon_j)\gamma_j}(x_j)\, dx\right). \tag{3}$$

Because $\deg_{x_j}(x_j^b f_j^{(b-\epsilon_j)\gamma_j}(x_j)) = (b-\epsilon_j)p+\epsilon_j$, we see from Equation (2) that $c_\tau u_j^{(b-\epsilon_j)\gamma_j/p} x_j^b y^{r-(b-\epsilon_j)\gamma_j} dx$ appears in Expression (3).

The coefficient c_τ in Expression (3) is nonzero because $r \leq p - 2$ for all $\omega \in H$. Also, $u_j \neq 0$ as it is the leading coefficient of $f_j(x_j)$. This term is canceled by no others. To see this, notice that the coefficient of $x_j^b y^{r-(b-\epsilon_j)\gamma_j} dx$ in Equation (1) is zero unless $\tau_{-1} = r - (b - \epsilon_j)\gamma_j$ and $\tau_j \geq (b - \epsilon_j)\gamma_j$. ∎

The next lemma shows that the coefficient of $\kappa(\mathcal{C}(\omega))$ is zero in $\mathcal{C}(\omega')$ for any 1-form $\omega' \in W$ which is smaller than ω.

Lemma 3.4. *If $\omega \in H$ and $\omega' \in W$ with $\omega' \prec \omega$, then the coefficient of $\kappa(\mathcal{C}(\omega))$ is zero in $\mathcal{C}(\omega')$.*

Proof. Write $\omega' = x_k^B y^R dx$ and recall the calculation:

$$\mathcal{C}\left(x_k^B y^R dx\right) = \sum_{\tau, |\tau|=R} c_\tau y^{\tau-1} \mathcal{C}\left(x_k^B f_0^{\tau_0}(x) f_1^{\tau_1}(x_1) \cdots f_m^{\tau_m}(x_m)\right). \quad (4)$$

Case 1: Suppose $\omega = x^b y^r dx \in H_0$. The claim is that the coefficient c_ω of $\kappa(\mathcal{C}(\omega)) = x^b y^{r-(b+1)\gamma_0} dx$ in Equation (4) is zero for any $\omega' \prec x^b y^r dx$. The coefficient c_ω will be zero unless $\tau_{-1} = r - (b+1)\gamma_0$. This gives the restriction that $\tau_0 \leq R - (r - (b+1)\gamma_0)$.

If $k = 0$, c_ω will be zero unless $\tau_0 d_0 + B \geq (b+1)p - 1$. Combining these inequalities yields that

$$R - r \geq (b - B)/d_0.$$

Because both b and B are less than $d_0 - 2$, c_ω is non-zero only if $R > r$ or if $R = r$ and $B \geq b$.

If $k \neq 0$, the coefficient c_ω of $x^b y^{r-(b+1)\gamma_0} dx$ in Equation (4) will be zero unless $\tau_0 d_0 - B \geq (b+1)p - 1$. Combining the given inequalities shows that

$$R - r \geq (b + B)/d_0.$$

As $B > 0$, this shows that c_ω is non-zero only if $R > r$. In both cases, $\omega' = x_k^B y^R dx \not\prec \omega = x^b y^r dx$.

Case 2: Suppose $\omega \in H_j$ for some $1 \leq j \leq m$. The claim is that the coefficient c_ω of the 1-form $x_j^b y^{r-(b-1)\gamma_j} dx$ in $\mathcal{C}(\omega')$ is zero for any $\omega' \prec x_j^b y^r dx$. The coefficient c_ω is non-zero only if $\tau_{-1} = r - (b-1)\gamma_j$. This gives the restriction that $\tau_j \leq R - (r - (b-1)\gamma_j)$.

If $k \neq j$, then c_ω is non-zero only if $\tau_j d_j \geq (b-1)p + 1$ and so

$$R - r \geq b/d_j.$$

As $b > 0$, c_ω is non-zero only if $R > r$.

If $k = j$, the coefficient c_ω is non-zero only if $\tau_j d_j + B \geq (b-1)p + 1$ which yields that

$$R - r \geq (b - B)/d_j.$$

Since b and B are both bounded by d_j, this is only satisfied if $R > r$ or if $R = r$ and $B \geq b$, in other words, only if $\omega' = x_k^B y^R dx \not\prec \omega = x^b y^r dx$. ☐

Proposition 3.5. *The columns of the Cartier-Manin matrix M corresponding to the 1-forms in H are linearly independent.*

Proof. This follows from Lemmas 3.3 and 3.4 since the key terms $\kappa(\mathcal{C}(\omega))$ yield pivots of M for $\omega \in H$. ☐

3.5 Linearly dependent columns of the Cartier-Manin matrix

In this section, we prove that the columns of the Cartier-Manin matrix associated with the 1-forms in A do not contribute to the rank of the Cartier-Manin matrix, because they are linearly dependent on the columns associated with the 1-forms in H.

For fixed j and r, let B vary and consider the ordered pair (B, R) of exponents in $\kappa(\mathcal{C}(x_j^B y^r dx)$. The points (B, R) lie on a line of slope $-\gamma_j$, specifically the line $R = r + \epsilon_j \gamma_j - \gamma_j B$, where $\epsilon_j = -1$ if $j = 0$ and $\epsilon_j = 1$ if $1 \leq j \leq m$. For $0 \leq j \leq m$ and $r \leq (p-2)/2$, let

$$Z_{j,r} = \left\{ x_j^B y^R dx \in W_j \mid R = r + \epsilon_j \gamma_j - \gamma_j B \right\}.$$

Note that $Z_{0,r}$ is empty if $0 \leq r < \gamma_0$. Let

$$Y_{j,r} = \begin{cases} \cup_{\ell=\gamma_0}^r Z_{0,\ell} & \text{if } j = 0, \\ \cup_{\ell=0}^r Z_{j,\ell} & \text{if } 1 \leq j \leq m. \end{cases}$$

Lemma 3.6. *Suppose $\eta = x_j^b y^r dx \in W_j$ for some $0 \le j \le m$ with $r \le (p-2)/2$. Then $\mathcal{C}(\eta) \in \mathrm{span}(Y_{i,r} \mid 0 \le i \le m)$.*

Proof. Fix $\sigma \in W_i$ with $0 \le i \le m$ and let c_σ denote the coefficient of σ in $\mathcal{C}(\eta)$. It suffices to show that $\sigma \in Y_{i,r}$ whenever $c_\sigma \ne 0$. Write $\sigma = x_i^B y^R dx$. By Equation (1), $c_\sigma = 0$ unless $\tau_{-1} = R$. This gives that $\tau_i \le r - R$. If $R \ge r + \epsilon_i\gamma_i - \gamma_i B + 1$ then $\tau_i \le \gamma_i B - \epsilon_i \gamma_i - 1$. The degree of x_i in $x_j^b f_i^{\tau_i}(x_i)$ satisfies

$$\begin{aligned} \deg_{x_i}\left(x_j^b f_i^{\tau_i}(x_i)\right) &\le b + \tau_i d_i \\ &\le b + (\gamma_i B - \epsilon_i\gamma_i - 1)\, d_i \\ &= (B - \epsilon_i)p - B + b + \epsilon_i - d_i. \end{aligned}$$

By the definition of W_i, if $i = 0$ then $b \le d_0 - 2$ and $B \ge 0$, and if $1 \le i \le m$ then $b \le d_i$ and $B \ge 1$. So, $\deg_{x_i}(x_j^b f_i^{\tau_i}(x_i)) < (B - \epsilon_i)p + \epsilon_i$. Thus, $c_\sigma = 0$ when $R > r + \epsilon_i\gamma_i - \gamma_i B$. □

Lemma 3.7. *Suppose $r \le (p-2)/2$ and $0 \le i \le m$. Every element of $Y_{i,r}$ is a key term of $\mathcal{C}(\omega)$ for some $\omega \in H_i$.*

Proof. Let $x_i^B y^R dx \in Y_{i,r}$. Define $\omega = x_i^B y^\rho dx$ where $\rho = R - \epsilon_i\gamma_i + \gamma_i B$. It suffices to show that $\omega \in H_i$, since $\kappa(\mathcal{C}(\omega)) = x_i^B y^R dx$. If $x_i^B y^R dx \in Y_{i,r}$ then $R \le r + \epsilon_i\gamma_i - \gamma_i B$, so $\rho \le r$. The 1-form $x_i^B y^\rho dx$ is in H_i because $B \ge 0$, and $-\epsilon_i\gamma_i + \gamma_i B \le \rho \le (p-2)/2$. □

Lemma 3.8. *If $\eta \in A$, then $\mathcal{C}(\eta)$ is contained in* $\mathrm{span}\{\mathcal{C}(\omega) \mid \omega \in H\}$.

Proof. Write $\eta = x_j^b y^r dx$ for some $0 \le j \le m$. Since $\eta \in A$, $r \le (p-2)/2$. By Lemma 3.6, $\mathcal{C}(\eta) \in \mathrm{span}(Y_{i,r} \mid 0 \le i \le m)$. By Lemma 3.7, $\mathcal{C}(\eta) \in \mathrm{span}\{\kappa(\mathcal{C}(\omega)) \mid \omega \in H\}$. Let $\omega^* = x_j^B y^R dx$ be the largest 1-form in H for which the coefficient of $\kappa(\mathcal{C}(\omega^*))$ in $\mathcal{C}(\eta)$ is non-zero. From the proof of Lemma 3.7, we see that $R < (p-2)/2$. Let $\nu \in k^\times$ be such that the coefficient of $\kappa(\mathcal{C}(\omega^*))$ is zero in $\mathcal{C}(\eta) - \nu\mathcal{C}(\omega^*)$. If τ is a monomial in $\mathcal{C}(\omega^*)$, then $\tau = \kappa(\mathcal{C}(\omega^{**}))$ for some $\omega^{**} \in H$. Lemma 3.4 implies that $\omega^{**} \prec \omega^*$. Therefore, the terms in $\mathcal{C}(\eta) - \nu\mathcal{C}(\omega^*)$ are key terms of $\mathcal{C}(\omega^{**})$ for $\omega^{**} \prec \omega^*$. Repeating this process shows that $\mathcal{C}(\eta)$ can be written as a linear combination $\sum_{\omega \in H} \nu_\omega \mathcal{C}(\omega)$. □

3.6 Main result

Theorem 3.9. *Let X be an Artin-Schreier curve with equation $y^p - y = f(x)$, with $f(x) \in k(x)$. Suppose $f(x)$ has $m+1$ poles, with orders $d_0, \dots, d_m$ and let $L = \mathrm{LCM}(d_0, \dots, d_m)$. If $p \equiv 1 \bmod L$, then the a-number of X is*

$$a_X = \sum_{j=0}^{m} a_j, \text{ where } a_j = \begin{cases} (p-1)d_j/4 & \text{if } d_j \text{ even,} \\ (p-1)(d_j-1)(d_j+1)/(4d_j) & \text{if } d_j \text{ odd.} \end{cases}$$

Proof. By Proposition 3.5 and Lemma 3.8, the rank of the Cartier-Manin matrix is equal to $\sum_{j=0}^m \#H_j$. Since $a = g - \mathrm{rank}(M)$ and $g = \#W$, this implies $a = \sum_{j=0}^m (\#W_j - \#H_j)$. It thus suffices to show that $\#W_j - \#H_j = a_j$ for the value of a_j as stated for $0 \le j \le m$.

Recall that $\#W_j = (p-1)(d_j + \epsilon_j)/2$. We will count the ordered pairs (b, r) corresponding to $x^b y^r dx \in H_j$. The lines $r = p - 2 + \epsilon_j\gamma_j - \gamma_j b$ and $r = \gamma_j b - \epsilon_j\gamma_j$ intersect at $b = d_j/2 + \epsilon_j - 1/2\gamma_j$. The largest value of b appearing in H_j is

$$b' = \begin{cases} d_j/2 + \epsilon_j - 1 & \text{if } d_j \text{ is even,} \\ d_j/2 + \epsilon_j - 1/2 & \text{if } d_j \text{ is odd.} \end{cases}$$

Let $b_j = 0$ if $j = 0$ and $b_j = 1$ if $j \neq 0$. Then

$$\begin{aligned}
a_j &= \#W_j - \#H_j \\
&= (p-1)(d_j+\epsilon_j)/2 - \sum_{b_j}^{b'} (p-1+2\epsilon_j\gamma_j - 2\gamma_j b) \\
&= (p-1)(d_j+\epsilon_j)/2 - (p-1+2\epsilon_j\gamma_j)(b' - b_j + 1) + 2\gamma_j b'\left(b'+1\right)/2 \\
&= \begin{cases} (p-1)d_j/4 & \text{if } d_j \text{ even}, \\ (p-1)(d_j-1)(d_j+1)/(4d_j) & \text{if } d_j \text{ odd}. \end{cases}
\end{aligned}$$

□

3.7 Open questions

Here are two questions that emerge from this work:

Question 1: Under the condition $p \equiv 1 \bmod L$, are the Ekedahl-Oort type and the Dieudonné module of the Jacobian of the Artin-Schreier curve $X : y^p - y = f(x)$ determined by the orders of the poles of $f(x)$?

Question 2: What are other families of curves for which the p-rank, Newton polygon, a-number, and Ekedahl-Oort type of the fibres of the family are constant?

For example, when $p = 2$, the Ekedahl-Oort type (and 2-rank and a-number) of an Artin-Schreier (hyperelliptic) curve depend only on the orders of the poles of $f(x)$ [8].

References

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

[2] Régis Blache. p-density, exponential sums and Artin-Schreier curves. arXiv: 0812.3382v1.

[3] Régis Blache, Éric Férard, and Hui June Zhu. Hodge-Stickelberger polygons for L-functions of exponential sums of $P(x^s)$. *Math. Res. Lett.*, 15(5):1053–1071, 2008.

[4] Pierre Cartier. Une nouvelle opération sur les formes différentielles. *Lecture Notes Ser. Comput.*, 244:426–428, 1957.

[5] Richard M. Crew. Etale p-covers in characteristic p. *Compositio Math.*, 52(1):31–45, 1984.

[6] Torsten Ekedahl. On supersingular curves and abelian varieties. *Math. Scand.*, 60(2):151–178, 1987.

[7] Arsen Elkin. The rank of the Cartier operator on cyclic covers of the projective line. *J. Algebra*, 327:1–12, 2011.

[8] Arsen Elkin and Rachel Pries. Ekedahl-Oort strata of hyperelliptic curves in characteristic 2. to appear in Algebra and Number Theory, arXiv:1007.1226.

[9] Darren Glass and Rachel Pries. Hyperelliptic curves with prescribed p-torsion. *Manuscripta Math.*, 117(3):299–317, 2005.

[10] Shushi Harashita. Ekedahl-Oort strata and the first Newton slope strata. *J. Algebraic Geom.*, 16(1):171–199, 2007.

[11] Shushi Harashita. Generic Newton polygons of Ekedahl-Oort strata: Oort's conjecture. *Ann. Inst. Fourier (Grenoble)*, 60(5):1787–1830, 2010.

[12] Alan G. B. Lauder and Daqing Wan. Computing zeta functions of Artin-Schreier curves over finite fields. *LMS J. Comput. Math.*, 5:34–55, 2002.

[13] Alan G. B. Lauder and Daqing Wan. Computing zeta functions of Artin-Schreier curves over finite fields. II. *J. Complexity*, 20(2-3):331–349, 2004.

[14] Ke-Zheng Li and Frans Oort. *Moduli of supersingular abelian varieties*, volume 1680 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1998.

[15] Enric Nart and Daniel Sadornil. Hyperelliptic curves of genus three over finite fields of even characteristic. *Finite Fields Appl.*, 10(2):198–220, 2004.

[16] Niels O. Nygaard. Slopes of powers of Frobenius on crystalline cohomology. *Ann. Sci. École Norm. Sup. (4)*, 14(4):369–401 (1982), 1981.

[17] Rachel Pries and Hui June Zhu. The p-rank stratification of Artin-Schreier curves. Annales de l'Institut Fourier, Vol. 62 no. 2 (2012), p. 707-726, math.NT/0609657v2.

[18] Rachel J. Pries. Jacobians of quotients of Artin-Schreier curves. In *Recent progress in arithmetic and algebraic geometry*, volume 386 of *Contemp. Math.*, pages 145–156. Amer. Math. Soc., Providence, RI, 2005.

[19] Antonio Rojas-León and Daqing Wan. Improvements of the Weil bound for Artin-Schreier curves. *Math. Ann.*, 351(2):417–442, 2011.

[20] Jasper Scholten and Hui June Zhu. Slope estimates of Artin-Schreier curves. *Compositio Math.*, 137(3):275–292, 2003.

[21] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

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

[23] Francis J. Sullivan. p-torsion in the class group of curves with too many automorphisms. *Arch. Math. (Basel)*, 26:253–261, 1975.

[24] Gerard van der Geer and Marcel van der Vlugt. On the existence of supersingular curves of given genus. *J. Reine Angew. Math.*, 458:53–61, 1995.

[25] Noriko Yui. On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$. *J. Algebra*, 52(2):378–410, 1978.

[26] Hui June Zhu. L-functions of exponential sums over one-dimensional affinoids: Newton over Hodge. *Int. Math. Res. Not.*, (30):1529–1550, 2004.

Shawn Farnell
Department of Mathematics, Kenyon College
Gambier, Ohio 43022, USA
farnells@kenyon.edu

Rachel Pries
Department of Mathematics, Colorado State University
Fort Collins, CO 80523-1874, USA
pries@math.colostate.edu