TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 368, Number 12, December 2016, Pages 8553–8595
http://dx.doi.org/10.1090/tran6641
Article electronically published on January 27, 2016

ARITHMETIC OF ABELIAN VARIETIES IN ARTIN-SCHREIER EXTENSIONS

RACHEL PRIES AND DOUGLAS ULMER

Abstract. We study abelian varieties defined over function fields of curves in positive characteristic p, focusing on their arithmetic in the system of Artin-Schreier extensions. First, we prove that the L-function of such an abelian variety vanishes to high order at the center point of its functional equation under a parity condition on the conductor. Second, we develop an Artin-Schreier variant of a construction of Berger. This yields a new class of Jacobians over function fields for which the Birch and Swinnerton-Dyer conjecture holds. Third, we give a formula for the rank of the Mordell-Weil groups of these Jacobians in terms of the geometry of their fibers of bad reduction and homomorphisms between Jacobians of auxiliary Artin-Schreier curves. We illustrate these theorems by computing the rank for explicit examples of Jacobians of arbitrary dimension g, exhibiting Jacobians with bounded rank and others with unbounded rank in the tower of Artin-Schreier extensions. Finally, we compute the Mordell-Weil lattices of an isotrivial elliptic curve and a family of non-isotrivial elliptic curves. The latter exhibits an exotic phenomenon whereby the angles between lattice vectors are related to point counts on elliptic curves over finite fields. Our methods also yield new results about supersingular factors of Jacobians of Artin-Schreier curves.

1. Introduction

Let k be a finite field of characteristic $p > 0$ and suppose $F = k(\mathcal{C})$ is the function field of a smooth, projective curve $\mathcal{C}$ over k. Given an abelian variety J defined over F, the Birch and Swinnerton-Dyer (BSD) conjecture relates the L-function of J and the Mordell-Weil group $J(F)$. In particular, it states that the algebraic rank of the Mordell-Weil group equals the analytic rank, the order of vanishing of the L-function at $s = 1$. If the BSD conjecture is true for J over F and if K/F is a finite extension, it is not known in general whether the BSD conjecture is true for J over K.

In [Ulm07], the second author studied the behavior of a more general class of L-functions over geometrically abelian extensions K/F. Specifically, for certain self-dual symplectic or orthogonal representations $\rho : G_F \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ of weight w, there is a factorization of $L(\rho, K, T)$, with factors indexed by orbits of the character group of $\mathrm{Gal}(K/F)$ under Frobenius, and a criterion for a factor to have a zero at the center point of its functional equation. Under a parity condition on the conductor of ρ, this implies that the order of vanishing of $L(\rho, K_d, T)$ at $T = |k|^{-(w+1)/2}$ is unbounded among Kummer extensions of the form $K_d = k(t^{1/d})$ of $F = k(t)$; see [Ulm07, Theorem 4.7].

Received by the editors June 10, 2013 and, in revised form, October 15, 2014.
2010 *Mathematics Subject Classification.* Primary 11G10, 11G40, 14G05; Secondary 11G05, 11G30, 14H25, 14J20, 14K15.

The system of rational Kummer extensions of function fields also plays a key role in the papers [Ber08, Ulm13a, Ulm14a]. For example, [Ber08] proves that the BSD conjecture holds for Jacobians J_X/K_d when X is in the class of curves defined by equations of the form $f(x) - tg(y)$ over $F = k(t)$ and K_d is in the Kummer tower of fields $K_d = k(t^{1/d})$. Also, [Ulm13a] gives a formula for the rank of J_X over K_d which depends on homomorphisms between the Jacobians of auxiliary Kummer curves.

In this paper, we study these phenomena for the system of Artin-Schreier extensions of function fields of positive characteristic. The main results are analogous to those described above: an unboundedness of analytic ranks result (Corollary 2.7.3), a proof of the BSD conjecture for Jacobians of a new class of curves X over an Artin-Schreier tower of fields (Corollary 3.1.4), and a formula for the rank of the Mordell-Weil group of J_X over Artin-Schreier extensions which depends on homomorphisms between the Jacobians of auxiliary Artin-Schreier curves (Theorem 5.2.1).

There are several reasons why the Artin-Schreier variants of these theorems are quite compelling. First, the curves which can be studied using the Artin-Schreier variant include those defined by an equation of the form $f(x)-g(y)-t$ over $F = k(t)$. The geometry of these curves is comparatively easy to analyze, allowing us to apply the main results in broad generality. For example, Proposition 4.4.1 illustrates that the hyperelliptic curve $x^2 = g(y) + t$ with $g(y) \in k[y]$ of degree N satisfies the BSD conjecture, with unbounded rank in the tower of Artin-Schreier extensions of $k(t)$, under the very mild conditions that $p \nmid N$ and the finite critical values of $g(y)$ are distinct. Second, the structure of endomorphism rings of Jacobians of Artin-Schreier curves is sometimes well understood. This allows us to compute the exact value of the rank of the Mordell-Weil group in several natural cases. Finally, some apparently unusual lattices appear as Mordell-Weil lattices of elliptic curves covered by our analysis. We illustrate this for the family of elliptic curves $Y^2 = X(X+16b^2)(X+t^2)$ (where b is a parameter in a finite field) in Subsection 7.3.

Here is an outline of the paper. In Section 2, we consider certain elementary abelian extensions K of $F = k(\mathcal{C})$ with $\deg(K/F) = q$ a power of p, and we study the L-functions $L(\rho, K, T)$ of certain self-dual representations $\rho : G_F \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$. Using results about Artin conductors of twists of ρ by characters of $\mathrm{Gal}(K/F)$, we prove a lower bound for the order of vanishing of $L(\rho, K, T)$ at the center point of the functional equation. In the case of an abelian variety J over F whose conductor satisfies a parity condition, this yields a lower bound for the order of vanishing of $L(J/K, s)$ at $s = 1$, Corollary 2.7.3.

In Section 3, we prove that a new class of surfaces has the DPCT property introduced by Berger. More precisely, we prove that a surface associated to the curve X given by an equation of the form $f(x)-g(y)-t$ over $F = k(t)$ is dominated by a product of curves and, furthermore, this DPC property is preserved under pullback to the field $K_q := F(u)/(u^q - u - t)$ for all powers q of p. It follows that the BSD conjecture holds for the Jacobians of this class of curves X over this Artin-Schreier tower of fields, Corollary 3.1.4. In Section 4, we combine the results from Sections 2 and 3 to give a broad array of examples of Jacobians over rational function fields $k(u)$ which satisfy the BSD conjecture and have large Mordell-Weil rank; see, e.g., Proposition 4.4.1.

Section 5 contains a formula for the rank of J_X over K_q in terms of the geometry of the fibers of bad reduction of X and the rank of the group of homomorphisms

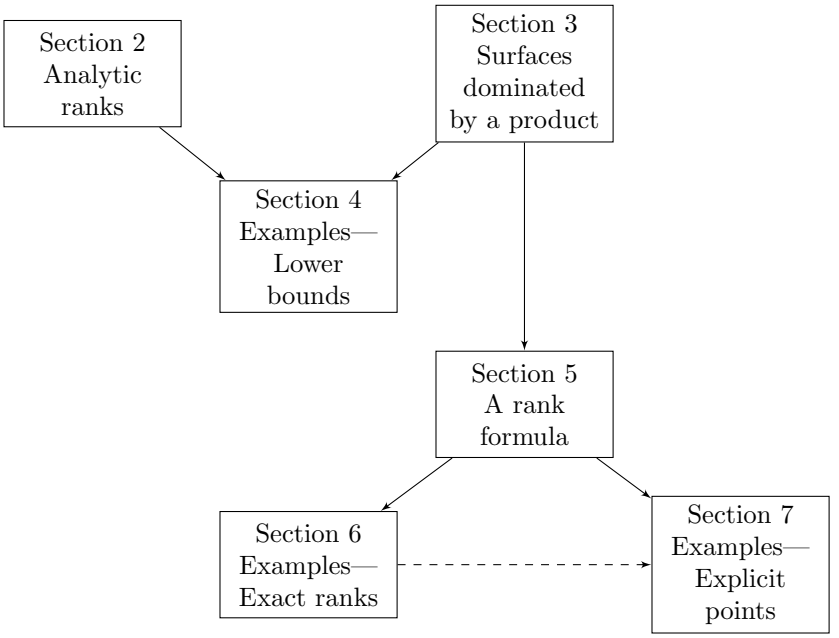

FIGURE 1. Leitfaden

between the Jacobians of auxiliary curves. (The auxiliary curves are $\mathcal{C}_q$ and $\mathcal{D}_q$, defined by equations $z^q - z = f(x)$ and $w^q - w = g(y)$, and we consider homomorphisms which commute with the $\mathbb{F}_q$-Galois actions on $\mathcal{C}_q$ and $\mathcal{D}_q$; see Theorem 5.2.1.) Section 6 contains three applications of the rank formula: first, by considering cases where $\mathcal{C}_q$ is ordinary and $\mathcal{D}_q$ has p-rank 0, we construct examples of curves X over F with arbitrary genus for which the rank of J_X over K_q is bounded independently of q; second, looking at the case when $f = g$, we construct examples of curves X over F with arbitrary genus for which the rank of X over K_q goes to infinity with q; third, we combine the lower bound for the analytic rank and the rank formula to deduce the existence of supersingular factors of Jacobians of Artin-Schreier curves.

Finally, in Section 7, we construct explicit points and compute heights for two examples. When $q \equiv 2 \bmod 3$, the isotrivial elliptic curve E defined by $Y^2 + tY = X^3$ has rank $2(q-1)$ over $K_q = \mathbb{F}_{q^2}(u)$ where $u^q - u = t$. We construct a subgroup of finite index in the Mordell-Weil group, and we conjecture that the index is $|Ш(E/K_q)|^{1/2}$ (which is known to be finite in this case). For $b \notin \{0, 1, -1\}$, the non-isotrivial curve $Y^2 = X(X + 16b^2)(X + t^2)$ has rank $q - 1$ over K_q, and again we construct a subgroup of finite index in the Mordell-Weil group. In this case, the lattice generated by $q - 1$ explicit points is in a certain sense a perturbation of the lattice A^*_{q-1} where the fluctuations are determined by point counts on another family of elliptic curves. This rather exotic situation has, to our knowledge, not appeared in print before.

An appendix, Section 8, collects all the results we need about ramification, Newton polygons, and endomorphism algebras of Artin-Schreier curves.

Figure 1 shows dependencies between the sections. A dashed line indicates a very mild dependency which can be ignored to first approximation, whereas a solid line indicates a more significant dependency. We have omitted dependencies in the appendix; these exist in Sections 2, 6, and 7, and at one place in Section 3.

2. Analytic ranks

In this section, we use results from [Ulm07] to show that analytic ranks are often large in Artin-Schreier extensions. The main result is Corollary 2.7.3.

2.1. **Notation.** Let p be a prime number, let $\mathbb{F}_p$ be the field of p elements, and let k be a finite field of characteristic p. We write $r = |k|$ for the cardinality of k. Let $F = k(\mathcal{C})$ be the function field of a smooth, projective, irreducible curve $\mathcal{C}$ over k. Let F^{sep} be a separable closure of F. We write $\overline{\mathbb{F}}_p$ for the algebraic closure of $\mathbb{F}_p$ in F^{sep}. Let $G_F = \mathrm{Gal}(F^{sep}/F)$ be the Galois group of F.

Let $\ell \neq p$ be a prime number and let $\overline{\mathbb{Q}}_\ell$ be an algebraic closure of the ℓ-adic numbers. Fix a representation $\rho : G_F \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ satisfying the hypotheses of [Ulm07, §4.2]. In particular, ρ is assumed to be self-dual of some weight w and sign $-\epsilon$. When $\epsilon = 1$ we say ρ is symplectic, and when $\epsilon = -1$ we say ρ is orthogonal.

The representation ρ gives rise to an L-function $L(\rho, F, T)$ given by an Euler product as in [Ulm07, §4.3]. We write $L(\rho, K, T)$ for $L(\rho|_{G_K}, K, T)$ for any finite extension K of F contained in F^{sep}.

In [Ulm07, §4], we studied the order of vanishing of $L(\rho, K, T)/L(\rho, F, T)$ at the center point $T = r^{-(w+1)/2}$ when K/F is a Kummer extension. Here we want to study the analogous order when K/F is an Artin-Schreier extension.

2.2. **Extensions.** Let q be a power of p and write $\wp_q(z)$ for the polynomial $z^q - z$. We will consider field extensions K of F of the form

$$K = K_{\wp_q, f} = F[z]/(\wp_q(z) - f) \tag{2.2.1}$$

for $f \in F \setminus k$. We assume throughout that $\overline{\mathbb{F}}_p K$ is a field, a condition which is guaranteed when f has a pole of order prime to p at some place of F. As described in Lemma 8.1.1, under this assumption, the degree q field extension K/F is "geometrically abelian" in the sense that $\overline{\mathbb{F}}_p K/\overline{\mathbb{F}}_p F$ is Galois with abelian Galois group. In fact, setting $H = \mathrm{Gal}(\overline{\mathbb{F}}_p K/\overline{\mathbb{F}}_p F)$, we have a canonical isomorphism $H \cong \mathbb{F}_q$, where $\mathbb{F}_q$ is the subfield of F^{sep} of cardinality q. The element $\alpha \in \mathbb{F}_q$ corresponds to the automorphism of $\overline{\mathbb{F}}_p K$ which sends the class of z in (2.2.1) to $z + \alpha$.

It will be convenient to consider a more general class of geometrically abelian extensions whose Galois groups are elementary abelian p-groups. Suppose that A is a monic, separable, additive polynomial, in other words a polynomial of the form

$$A(z) = z^{p^\nu} + \sum_{i=0}^{\nu-1} a_i z^{p^i}$$

with $a_i \in \overline{\mathbb{F}}_p$ and $a_0 \neq 0$. We will see in Subsection 8.2 that there is a bijection between such polynomials A and subgroups of $\overline{\mathbb{F}}_p$ which associates to A the group H_A of its roots. The field generated by the coefficients of A is the field of p^μ elements, where p^μ is the smallest power of p such that H_A is stable under the p^μ-power Frobenius.

Suppose $f \in F$ has a pole of order prime to p at some place of F and that A has coefficients in k. Then we have a field extension

$$K = K_{A,f} = F[x]/(A(z) - f).$$

It is geometrically Galois over F, with $\mathrm{Gal}(\overline{\mathbb{F}}_p K/\overline{\mathbb{F}}_p F)$ canonically isomorphic to H_A.

By Lemma 8.2.2, if A has roots in $\mathbb{F}_q$, then there exists another monic, separable, additive polynomial B such that the composition $A \circ B$ equals $\wp_q$. Furthermore, this implies that $K_{A,f}$ is a subfield of $K_{\wp_q,f}$ and that $\mathrm{Gal}(\overline{\mathbb{F}}_p K_{A,f}/\overline{\mathbb{F}}_p F)$ is a quotient of $\mathbb{F}_q$, namely $B(\mathbb{F}_q)$. In particular, for many questions, we may reduce to the case where $K_{A,f}$ is the Artin-Schreier extension $K_{\wp_q,f}$.

2.3. **Characters.** Let $K = K_{\wp_q,f}$ be an Artin-Schreier extension of F as in Subsection 2.2, and let $H = \mathrm{Gal}(\overline{\mathbb{F}}_p K/\overline{\mathbb{F}}_p F) \cong \mathbb{F}_q$. Fix once and for all a non-trivial additive character $\psi_0 : \mathbb{F}_p \to \overline{\mathbb{Q}}_\ell^{\times}$. Let $\hat{H} = \mathrm{Hom}(H, \overline{\mathbb{Q}}_\ell^{\times})$ be the group of $\overline{\mathbb{Q}}_\ell$-valued characters of H. Then we have an identification $\hat{H} \cong \mathbb{F}_q$ under which $\beta \in \mathbb{F}_q$ corresponds to the character $\chi_\beta : H \to \overline{\mathbb{Q}}_\ell^{\times}$, $\alpha \mapsto \psi_0(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha\beta))$.

Next we consider actions of $G_k = \mathrm{Gal}(\overline{k}/k)$ on H and $\hat{H}$. To define them, consider the natural projection $G_F \to G_k$, and let Φ be any lift of the (arithmetic) generator of G_k, namely the r-power Frobenius. Using this lift, G_k acts on $H = \mathrm{Gal}(\overline{\mathbb{F}}_p K/\overline{\mathbb{F}}_p F)$ on the left by conjugation, and it is easy to see that under the identification $H \cong \mathbb{F}_q$, Φ acts on $\mathbb{F}_q$ via the r-th power Frobenius.

We also have an action of G_k on $\hat{H}$ on the right by precomposition: $(\chi_\beta)^\Phi(\alpha) = \chi_\beta(\Phi(\alpha)) = \chi_\beta(\alpha^r)$. Since

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha^r\beta) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha\beta^{r^{-1}})$$

we see that $(\chi_\beta)^\Phi = \chi_{\beta^{r^{-1}}}$.

If A is a monic, separable, additive polynomial with coefficients in k and group of roots H_A, then the character group of H_A is naturally a subgroup of $\hat{H}$, and it is stable under the r-power Frobenius. More precisely, by Lemma 8.2.2(2), H_A is the quotient $B(\mathbb{F}_q)$ of $\mathbb{F}_q$, and so its character group is identified with $(\ker B)^\perp = (\mathrm{Im}\, A)^\perp$ where the orthogonal complements are taken with respect to the trace pairing $(x, y) \mapsto \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(xy)$.

As seen in Example 8.2.3, if r is a power of an odd prime p and $A(z) = z^{r^\nu} + z$, then the group H_A of roots of A generates $\mathbb{F}_q$ where $q = r^{2\nu}$. In this case, $A \circ B = \wp_q$ when $B = \wp_{r^\nu}$. If $f \in F$ has a pole of order prime to p at some place of F, then the field extension $K_{A,f}$ is a subextension of $K_{\wp_q,f}$ and its character group is identified with $(\ker B)^\perp = H_A$.

2.4. **Ramification and conductor.** We fix a place v of F and consider a decomposition subgroup G_v of $G = G_F$ at the place v and its inertia subgroup I_v.

Recall from [Ser79, Chap. IV] that the upper numbering of ramification groups is compatible with passing to a quotient, and so defines a filtration on the inertia group I_v, which we denote by I_v^t for real numbers $t \geq 0$. By the usual convention, we set $I_v^t = I_v$ for $-1 < t \leq 0$.

Let $\rho : G_F \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ be a Galois representation as above, acting on $V = \overline{\mathbb{Q}}_\ell^{\,n}$. We denote the local exponent at a place v of the conductor of ρ by $f_v(\rho)$. We refer to [Ser70] for the definition.

Now let $\chi : G_F \to \overline{\mathbb{Q}}_\ell^{\times}$ be a finite order character. We say "χ is more deeply ramified than ρ at v" if there exists a non-negative real number t such that $\rho(I_v^t) = \{id\}$ and $\chi(I_v^t) \neq \{id\}$. In other words, χ is non-trivial further into the ramification filtration than ρ is. Let t_0 be the largest number such that χ is non-trivial on $I_v^{t_0}$ and recall that $f_v(\chi) = 1 + t_0$ [Ser79, VI, §2, Proposition 5].

Lemma 2.4.1. *If χ is more deeply ramified than ρ at v, then*

$$f_v(\rho \otimes \chi) = \deg(\rho)\mathfrak{f}_v(\chi).$$

Proof. This is an easy exercise and presumably well known to experts. It is asserted in [DD13, Lemma 9.2(3)], and a detailed argument is given in [Ulm13b]. □

A particularly useful case of the lemma occurs when ρ is tamely ramified and χ is wildly ramified, e.g., when χ is an Artin-Schreier character.

2.5. **Factoring $L(\rho, K, T)$.** Fix a monic, separable, additive polynomial A with coefficients in k and a function $f \in F$ such that f has a pole of order prime to p at some place of F. Let $K = K_{A,f}$ be the corresponding extension whose geometric Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_p K/\overline{\mathbb{F}}_p F)$ is canonically identified with the group $H = H_A$ of roots of A. Let $\mathbb{F}_q$ be the subfield of F^{sep} generated by H_A. Recall the Galois representation ρ fixed above. In this section, we record a factorization of the L-function $L(\rho, K, T)$.

In Subsection 2.3 above, we identified the character group of H with a subgroup of $\mathbb{F}_q$ which is stable under the r-power Frobenius. As in [Ulm07, §3], we write $o \subset \hat{H} \subset \mathbb{F}_q$ for an orbit of the action of Fr_r. Note that the cardinality of the orbit o through $\beta \in \mathbb{F}_q$ is equal to the degree of the field extension $k(\beta)/k$ and is therefore at most 2ν.

As in [Ulm07, §4.4], we have a factorization

$$L(\rho, K, T) = \prod_{o \subset \hat{H}} L(\rho \otimes \sigma_o, F, T)$$

and a criterion for the factor $L(\rho \otimes \sigma_o, F, T)$ to have a zero at $T = \epsilon r^{-(w+1)/2}$ (or more generally to be divisible by a certain polynomial).

To unwind that criterion, we need to consider self-dual orbits. More precisely, note that the inverse of χ_β is $(\chi_\beta)^{-1} = \chi_{-\beta}$. Thus an orbit o is self-dual in the sense of [Ulm07, §3.4] if and only if there exists a positive integer ν such that $\beta^{r^\nu} = -\beta$ for all $\beta \in o$. The trivial orbit $o = \{0\}$ is of course self-dual in this sense. To ensure that that there are many other self-dual orbits, we may assume r is odd and take $A(x) = x^{r^\nu} + x$ for some positive integer ν. Then if β is a non-zero root of A, the orbit through β is self-dual. Since the size of this orbit is at most 2ν, we see that there are at least $(r^\nu - 1)/(2\nu)$ non-trivial self-dual orbits in this case.

We also note that if $\beta \neq 0$, then the order of the character χ_β is p, and since we are assuming r, and thus p, is odd, we have that χ_β has order > 2. Summarizing, we have the following.

Lemma 2.5.1. *Let k be a finite field of cardinality r and characteristic $p > 2$. Suppose $A(z) = z^{r^\nu} + z$. Suppose $f \in F$ has a pole of order prime to p, and let $K = K_{A,f}$. Let ρ be a representation of G_F as in Subsection* 2.1. *Then we have a factorization*

$$L(\rho, K, T) = \prod_{o \subset \hat{H}} L(\rho \otimes \sigma_o, F, T)$$

where the product is over the orbits of the r-power Frobenius on the roots of A. Aside from the orbit $o = \{0\}$, there are at least $(r^\nu - 1)/2\nu$ orbits, each of which is self-dual, has cardinality at most 2ν, and consists of characters of order $p > 2$.

2.6. **Parity conditions.** According to [Ulm07, Thm. 4.5], $L(\rho \otimes \sigma_o, F, T)$ vanishes at $T = r^{-(w+1)/2}$ if ρ is symplectic of weight w, o is a self-dual orbit, and the degree of $\mathrm{Cond}(\rho \otimes \chi_\beta)$ is odd for one, and therefore for all, $\beta \in o$. Thus to obtain a large order of vanishing, we should arrange matters so that $\rho \otimes \chi_\beta$ satisfies the conductor parity condition for many orbits o. This is not hard to do using Lemma 2.4.1.

Indeed, let S be the set of places where χ_β is ramified, and suppose that χ_β is more deeply ramified than ρ at each $v \in S$. Suppose also that $\sum_{v \notin S} f_v(\rho) \deg(v)$ is odd. Then using Lemma 2.5.1 we have

$$\deg \mathrm{Cond}(\rho \otimes \chi_\beta) = \sum_{v \in S} \deg(\rho) f_v(\chi_\beta) \deg(v) + \sum_{v \notin S} f_v(\rho) \deg(v).$$

Since ρ is symplectic, it has even degree, and so our assumptions imply that $\deg \mathrm{Cond}(\rho \otimes \chi_\beta)$ is odd.

2.7. **High ranks.** Putting everything together, we get results guaranteeing large analytic ranks in Artin-Schreier extensions:

Theorem 2.7.1. *Let k be a finite field of cardinality r and characteristic $p > 2$. Let $\nu \in \mathbb{N}$ and let k' be the field of $q = r^{2\nu}$ elements. Let $F = k(\mathcal{C})$ and $\rho : G_F \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ be as in Subsection 2.1. Assume that ρ is symplectically self-dual of weight w. Choose $f \in F$ with at least one pole of order prime to p. Suppose that either (1) $K = K_{A,f}$ where $A(z) = z^{r^\nu} + z$ or (2) $K = K_{\wp_q, f}$ where $\wp_q(z) = z^q - z$ as in Subsection 2.2. Let S be a set of places of F where K/F is ramified and suppose that ρ is at worst tamely ramified at each place $v \in S$. Suppose also that $\sum_{v \notin S} f_v(\rho) \deg(v)$ is odd. Then*

$$\mathrm{ord}_{s=(w+1)/2} \frac{L(\rho, K, s)}{L(\rho, F, s)} \geq (r^\nu - 1)/(2\nu)$$

and

$$\mathrm{ord}_{s=(w+1)/2} \frac{L(\rho, k'K, s)}{L(\rho, k'F, s)} \geq (r^\nu - 1).$$

Proof. For case (1), the first inequality is an easy consequence of the preceding subsections and [Ulm07, Thm. 4.5]. Indeed, by Lemma 2.5.1, we have a factorization

$$L(\rho, K, T) = \prod_{o \subset \hat{H}} L(\rho \otimes \sigma_o, F, T)$$

where the product is over the orbits of the r-power Frobenius on the roots of A. The factor on the right corresponding to the orbit $o = \{0\}$ is just $L(\rho, F, T)$, and by the lemma, all the other orbits are self-dual and consist of characters of order > 2. The hypotheses on the ramification of ρ allow us to apply Lemma 2.4.1 to conclude that the parity of $\deg \mathrm{Cond}(\rho \otimes \chi_\beta)$ is odd for all roots $\beta \neq 0$ of A. Thus [Ulm07, Thm. 4.5] implies that each of the factors $L(\rho \otimes \sigma_o, F, T)$ is divisible by $1 - (r^{(w+1)/2} T)^{|o|}$ and, in particular, has a zero at $T = r^{-(w+1)/2}$. Since there are $(r^\nu - 1)/2\nu$ non-trivial orbits, we obtain the desired lower bound.

Over any extension k' of k of degree divisible by 2ν, we have a further factorization

$$L(\rho \otimes \sigma_o, k'F, T) = \prod_{\beta \in o} L(\rho \otimes \chi_\beta, k'F, T),$$

and each factor $L(\rho \otimes \chi_\beta, k'F, T)$ is divisible by $(1 - |k'|^{(w+1)/2}T)$ and thus vanishes at $s = (w+1)/2$. This establishes the second lower bound in case (1).

The lower bounds for case (2) are an immediate consequence of those for case (1) since $K_{A,f}$ is a subextension of $K_{\wp_q,f}$ by Example 8.2.3. □

Remark 2.7.2. If $F = \mathbb{F}_p(t)$ and $f = t$, then the Artin-Schreier extension given by $u^q - u = t$ is again a rational function field. Thus starting with a suitable ρ and taking a large degree Artin-Schreier extension, or by taking multiple extensions, we obtain another proof of unbounded analytic ranks over the fixed ground field $\mathbb{F}_p(u)$.

As an illustration, we specialize Theorem 2.7.1 to the case where ρ is given by the action of G_F on the Tate module of an abelian variety over F.

Corollary 2.7.3. *Let k be a finite field of cardinality r and characteristic $p > 2$. Let $\nu \in \mathbb{N}$ and let k' be the field of $q = r^{2\nu}$ elements. Suppose J is an abelian variety over a function field $F = k(\mathcal{C})$ as in Subsection* 2.1. *Choose $f \in F$ with at least one pole of order prime to p. Suppose that either* (1) *$K = K_{A,f}$ where $A(z) = z^{r^\nu} + z$ or* (2) *$K = K_{\wp_q,f}$ where $\wp_q(z) = z^q - z$ as in Subsection* 2.2. *Let S be the set of places of F where K/F is ramified. Suppose that J is at worst tamely ramified at all places in S and that the degree of the part of the conductor of J away from S is odd. Then*

$$\operatorname{ord}_{s=1} L(J/K, s) \geq (r^\nu - 1)/(2\nu)$$

and

$$\operatorname{ord}_{s=1} L(J/k'K, s) \geq (r^\nu - 1).$$

2.8. **Orthogonal ρ and supersingularity.** Consider the set-up of Theorem 2.7.1, except that we assume that ρ is orthogonally self-dual instead of symplectically self-dual, and we replace the parity condition there with the assumption that

$$\deg(\rho) \sum_{v \in S} (-\operatorname{ord}_v(f) + 1) \deg(v) + \sum_{v \notin S} f_v(\rho) \deg(v)$$

is odd. Then [Ulm07, Thm. 4.5] implies that if o is an orbit with $o \neq \{0\}$, then $L(\rho \otimes \sigma_o, F, T)$ is divisible by $1 + (r^{(w+1)/2}T)^{|o|}$. In particular, over a large enough finite extension k' of k, at least $r^\nu - 1$ of the inverse roots of the L-function $L(\rho, K, T)/L(\rho, F, T)$ are equal to $|k'|^{(w+1)/2}$.

We apply this result to the case when ρ is the trivial representation to conclude that the Jacobians of certain Artin-Schreier curves have many copies of a supersingular elliptic curve as isogeny factors. This implies that the slope $1/2$ occurs with high multiplicity in their Newton polygons as defined in Subsection 8.3. However, as explained in Subsection 8.4, the occurrence of slope $1/2$ in the Newton polygon of an abelian variety usually does not give any information about whether the abelian variety has a supersingular elliptic curve as an isogeny factor. This gives the motivation for this result. More precisely:

Proposition 2.8.1. *With the notation of Corollary* 2.7.3, *write*

$$\operatorname{div}_\infty(f) = \sum_{i=1}^{m} a_i P_i$$

where the P_i are distinct $\overline{k}$-valued points of $\mathcal{C}$. Assume that $p \nmid a_i$ for all i and that $\sum_{i=1}^{m}(a_i+1)$ is odd. Let $\mathcal{J}$ (resp. $\mathcal{J}_{A,f}$, $\mathcal{J}_{\wp_q,f}$) be the Jacobian of $\mathcal{C}$ (resp. the cover $\mathcal{C}_{A,f}$ of $\mathcal{C}$ defined by $A(z)=f$, the cover $\mathcal{C}_{\wp_q,f}$ of $\mathcal{C}$ defined by $\wp_q(z)=f$). Then up to isogeny over $\overline{k}$, the abelian varieties $\mathcal{J}_{A,f}/\mathcal{J}$ and $\mathcal{J}_{\wp_q,f}/\mathcal{J}$ each contain at least $(r^\nu-1)/2$ copies of a supersingular elliptic curve.

Proof. We give only a brief sketch, since this result plays a minor role in the rest of the paper. An argument parallel to that in the proof of Theorem 2.7.1 shows that the numerator of the zeta function of $\mathcal{C}_{A,f}$ divided by that of $\mathcal{C}$ is divisible by

$$\left(1+r^\nu T^{2\nu}\right)^{(r^\nu-1)/(2\nu)}.$$

Thus over a large extension k' of k, at least $r^\nu-1$ of the inverse roots of the zeta function are equal to $|k'|^{1/2}$. Honda-Tate theory then shows that the Jacobian has a supersingular elliptic curve as an isogeny factor with multiplicity at least $(r^\nu-1)/2$. □

We will see in Section 8 that the lower bound of Proposition 2.8.1 is not always sharp.

2.9. **The case $p=2$.** The discussion of the preceding subsections does not apply when $p=2$ since in that case all characters of H have order 2. To get high ranks when $p=2$, we can use the variant of [Ulm07, Thm. 4.5] suggested in [Ulm07, 4.6]. In this variant, instead of symmetric or skew-symmetric matrices, we have orthogonal matrices, and zeroes are forced because 1 is always an eigenvalue of an orthogonal matrix of odd size, and ±1 are always eigenvalues of an orthogonal matrix of even size and determinant -1. The details are somewhat involved and tangential to the main concerns of this paper, so we will not include them here.

2.10. **Artin-Schreier-Witt extensions.** The argument leading to Theorem 2.7.1 generalizes easily to the situation where we replace Artin-Schreier extensions with Artin-Schreier-Witt extensions. This generalization is relevant even if $p=2$. We sketch very roughly the main points.

Let $W_n(F)$ be the ring of Witt vectors of length n with coefficients in F. We choose $\mathbf{f}\in W_n(F)$ and we always assume that its first component f_1 is such that x^q-x-f_1 is irreducible in $F[x]$ and so defines an extension of F of degree q. Then adjoining to F the solutions (in $W_n(F^{sep})$) of the equation $\mathrm{Fr}_q(\mathbf{x})-\mathbf{x}=\mathbf{f}$ yields a field extension of F which is geometrically Galois with group $W_n(\mathbb{F}_q)$. The character group of this Galois group can be identified with $W_n(\mathbb{F}_q)$, and we have an action of G_k (i.e., the r-power Frobenius where $r=|k|$) on the characters of this group.

Choose a positive integer ν and consider the situation above where $q=r^{2\nu}$. We claim that there are $r^{n\nu}$ solutions in $W_n(\mathbb{F}_q)$ to the equation $\mathrm{Fr}_{r^\nu}(\mathbf{x})+\mathbf{x}=0$. For $p>2$, this is clear—just take Witt vectors whose entries satisfy $x^{r^\nu}+x=0$. For $p=2$, the entries of $-\mathbf{x}$ are messy functions of those of $\mathbf{x}$, so we give a different argument. Namely, let us proceed by induction on n. For $n=1$, $\mathbf{x}_1=(1)$ is a solution. Suppose that $\mathbf{x}_{n-1}=(a_1,\dots,a_{n-1})$ satisfies $\mathrm{Fr}_{r^\nu}(\mathbf{x})+\mathbf{x}=0$. Then we have

$$\mathrm{Fr}_{r^\nu}(a_1,\dots,a_{n-1},0)+(a_1,\dots,a_{n-1},0)=(0,\dots,0,b_n),$$

and it is easy to see that b_n lies in the field of r^ν elements. We can thus solve the equation $a_n^{r^\nu}+a_n=b_n$, and then $\mathbf{x}_n=(a_1,\dots,a_n)$ solves $\mathrm{Fr}_{r^\nu}(\mathbf{x}_n)+\mathbf{x}_n=0$. With

one solution which is a unit in $W_n(\mathbb{F}_q)$ in hand, we remark that any multiple of our solution by an element of $W_n(\mathbb{F}_{r^\nu})$ is another solution, so we have $r^{n\nu}$ solutions in all.

Next we note that the self-dual orbits $o \subset W_n(\mathbb{F}_q)$ (i.e., those orbits stable under $\mathbf{x} \mapsto -\mathbf{x}$) are exactly the orbits whose elements satisfy $\mathrm{Fr}_{r^\nu}(\mathbf{x}) + \mathbf{x} = 0$. These orbits are of size at most 2ν. If $p > 2$, all but the orbit $o = \{0\}$ consist of characters of order > 2, whereas if $p = 2$, all but p^ν of the orbits consist of characters of order > 2. Thus taking $p > 2$ or $p = 2$ and $n > 1$, we have a plentiful supply of orbits which are self-dual and consist of characters of order > 2.

The last ingredient needed to ensure a high order of vanishing for the L-function is a conductor parity condition. This can be handled in a manner quite parallel to the cases considered in Subsection 2.6. Namely, we choose $\mathbf{f} \in W_n(F)$ so that at places where ρ and characters χ are ramified, χ should be so more deeply, and the remaining part of the conductor of ρ should have odd degree. Then $\rho \otimes \chi$ will have conductor of odd degree.

3. Surfaces dominated by a product of curves in Artin-Schreier towers

In this section, we extend a construction of Berger to another class of surfaces, following [Ulm13a, §§4-6].

3.1. **Construction of the surfaces.** Let k be a field with $\mathrm{Char}(k) = p$ and let $K = k(t)$. Suppose $\mathcal{C}$ and $\mathcal{D}$ are smooth projective irreducible curves over k. Suppose $f : \mathcal{C} \to \mathbb{P}^1$ and $g : \mathcal{D} \to \mathbb{P}^1$ are non-constant separable rational functions. Write the polar divisors of f and g as

$$\mathrm{div}_\infty(f) = \sum_{i=1}^{m} a_i P_i \quad \text{and} \quad \mathrm{div}_\infty(g) = \sum_{j=1}^{n} b_j Q_j$$

where the P_i and the Q_j are distinct $\overline{k}$-valued points of $\mathcal{C}$ and $\mathcal{D}$. Let

$$M = \sum_{i=1}^{m} a_i \quad \text{and} \quad N = \sum_{j=1}^{n} b_j.$$

We make the following *standing assumption*:

$$p \nmid a_i \text{ for } 1 \le i \le m \quad \text{and} \quad p \nmid b_j \text{ for } 1 \le j \le n. \tag{3.1.1}$$

We use the notation $\mathbb{P}^1_{k,t}$ to denote the projective line over k with a chosen parameter t. Define a rational map $\psi_1 : \mathcal{C} \times_k \mathcal{D} \dashrightarrow \mathbb{P}^1_{k,t}$ by the formula $t = f(x) - g(y)$ or more precisely

$$\psi_1(x,y) = \begin{cases} [f(x) - g(y) : 1] & \text{if } x \notin \{P_i\} \text{ and } y \notin \{Q_j\}, \\ [1:0] & \text{if } x \in \{P_i\} \text{ and } y \notin \{Q_j\}, \\ [1:0] & \text{if } x \notin \{P_i\} \text{ and } y \in \{Q_j\}. \end{cases}$$

The map ψ_1 is undefined at each of the points in the set

$$\mathbb{B} = \{(P_i, Q_j) \mid 1 \le i \le m, 1 \le j \le n\}.$$

Let $U = \mathcal{C} \times_k \mathcal{D} - \mathbb{B}$ and note that the restriction $\psi_1|_U : U \to \mathbb{P}^1_{k,t}$ is a morphism. We call the points in $\mathbb{B}$ "base points" because they are the base points of the pencil of divisors on $\mathcal{C} \times_k \mathcal{D}$ defined by ψ_1. Namely, for each closed point $v \in \mathbb{P}^1_{k,t}$, let

$\overline{\psi_1^{-1}(v)}$ denote the Zariski closure in $\mathcal{C} \times_k \mathcal{D}$ of $(\psi_1|_U)^{-1}(v)$. The points in $\mathbb{B}$ lie in each member of this family of divisors.

We note that the fiber of ψ_1 over $v = \infty$ is a union of horizontal and vertical divisors:

$$\overline{\psi_1^{-1}(\infty)} = \left(\bigcup_{i=1}^{m} \{a_i P_i\} \times \mathcal{D}\right) \cup \left(\bigcup_{j=1}^{n} \mathcal{C} \times \{b_j Q_j\}\right).$$

In particular, the complement of this divisor in $\mathcal{C} \times \mathcal{D}$ is again a product of (open) curves. This is the underlying geometric reason why the open sets considered in Proposition 3.1.3 below are dominated by products of curves, and ultimately why we are able to deduce the Tate and BSD conjectures in Theorem 3.1.2 below.

Suppose $\phi_1 : \mathcal{X} \to \mathcal{C} \times_k \mathcal{D}$ is a blow-up such that the composition $\pi_1 = \psi_1 \circ \phi_1 : \mathcal{X} \to \mathcal{C} \times_k \mathcal{D} \dashrightarrow \mathbb{P}^1_{k,t}$ is a generically smooth morphism. The statement of Theorem 3.1.2 below is independent of the choice of ϕ_1. In Proposition 3.1.5, we will construct a specific blow-up ϕ_1 in order to compute the genus of X in terms of the orders of the poles of f and g. We will use this construction later in Section 5 to find a formula for the rank of the Mordell-Weil group of the Jacobian of X.

Let $X \to \operatorname{Spec}(K)$ be the generic fiber of π_1 so that X is a smooth curve over $K = k(t)$. In Theorem 3.1.2, we show that $\mathcal{X}$ is dominated by a product of curves and X is irreducible over $\overline{k}K \simeq \overline{k}(t)$, thus proving the Tate conjecture for $\mathcal{X}$ and the BSD conjecture for the Jacobian of X when k is a finite field.

More generally, we prove analogous results for the entire system of rational Artin-Schreier extensions of $k[t]$. Let q be a power of p and set $\wp_q(u) = u^q - u$. We write $\mathcal{Y}_q = \mathbb{P}^1_{k,u}$ and we define a covering $\mathcal{Y}_q \to \mathbb{P}^1_{k,t}$ by setting $t = \wp_q(u)$. We write K_q for the function field of $\mathcal{Y}_q$, so that $K_q \cong k(u)$ and $K_q/k(t)$ is an extension of degree q. When the ground field k contains $\mathbb{F}_q$, then $K_q/k(t)$ is an $\mathbb{F}_q$-Galois extension.

Consider the base change:

$$\begin{array}{ccccc} \mathcal{S}_q := & \mathcal{Y}_q \times_{\mathbb{P}^1_{k,t}} \mathcal{X} & \to & \mathcal{X} \\ & \downarrow & & \downarrow \\ & \mathcal{Y}_q & \longrightarrow & \mathbb{P}^1_{k,t}. \end{array}$$

Because both $\mathcal{Y}_q$ and $\mathcal{X}$ have critical points over ∞, the fiber product $\mathcal{S}_q$ will usually not be smooth over k, or even normal. Let $\phi_q : \mathcal{X}_q \to \mathcal{S}_q$ be a blow-up of the normalization of $\mathcal{S}_q$ such that $\mathcal{X}_q$ is smooth over k. The statement of Theorem 3.1.2 is independent of the choice of ϕ_q. Let $\pi_q : \mathcal{X}_q \to \mathcal{Y}_q$ be the composition and let $X_q \to \operatorname{Spec}(K_q)$ be its generic fiber. Note that $X_q \cong X \times_{\operatorname{Spec} K} \operatorname{Spec}(K_q)$.

Theorem 3.1.2. *Given data k, $\mathcal{C}$, $\mathcal{D}$, f, g, and q as above, consider the fibered surface $\pi_q : \mathcal{X}_q \to \mathcal{Y}_q$ and the curve X_q/K_q constructed as above. Then:*

1. *$\mathcal{X}_q$ is dominated by a product of curves.*
2. *X_q is irreducible and remains irreducible over $\overline{k}K_q \cong \overline{k}(u)$.*
3. *If k is finite, the Tate conjecture holds for $\mathcal{X}_q$, and the BSD conjecture holds for the Jacobian of X_q.*

These results also hold for $\mathcal{X}$ and X.

The Tate conjecture mentioned in part (3) of Theorem 3.1.2 refers to Tate's second conjecture, $\operatorname{Rank} \operatorname{NS}(\mathcal{X}_q) = -\operatorname{ord}_{s=1} \zeta(\mathcal{X}, s)$, stated in [Tat65]. The BSD conjecture mentioned in part (3) of Theorem 3.1.2 and in Corollary 3.1.4 refers both to the basic BSD conjecture, $\operatorname{Rank}(J_{X_q}(K_q)) = \operatorname{ord}_{s=1} L(J_{X_q}/K_q, s)$ and the

refined BSD conjecture relating the leading coefficient of the L-function to other arithmetic invariants; see [Tat66b]. See also [Ulm14b, 6.1.1, 6.2.3, and 6.2.5] for further discussion of these conjectures.

We now introduce some notation useful for proving Theorem 3.1.2. Let $\mathcal{C}_q$ be the smooth projective irreducible curve covering $\mathcal{C}$ defined by $\wp_q(z) = f$ and let $\mathcal{D}_q$ be the smooth, projective irreducible curve covering $\mathcal{D}$ defined by $\wp_q(w) = g$. The morphisms $\mathcal{C}_q \to \mathcal{C}$ and $\mathcal{D}_q \to \mathcal{D}$ are geometric $\mathbb{F}_q$-Galois covers; i.e., after extending the ground field to $\overline{k}$, these covers are Galois and there is a canonical identification of the Galois group with $\mathbb{F}_q$.

Let $\mathcal{C}^\circ \subset \mathcal{C}$ and $\mathcal{C}_q^\circ \subset \mathcal{C}_q$ be the complements of the points above the poles of f. Similarly, let $\mathcal{D}^\circ \subset \mathcal{D}$ and $\mathcal{D}_q^\circ \subset \mathcal{D}_q$ be the complements of the points above the poles of g. Then $\mathcal{C}_q^\circ \to \mathcal{C}^\circ$ and $\mathcal{D}_q^\circ \to \mathcal{D}^\circ$ are étale geometric $\mathbb{F}_q$-Galois covers. Let $\mathcal{X}^o = \mathcal{C}^o \times \mathcal{D}^o$, and let $\mathcal{X}_q^\circ \subset \mathcal{X}_q$ be the complement of $\pi_q^{-1}(\infty_{\mathcal{Y}_q})$.

Proposition 3.1.3. *For each power q of p, there is a canonical isomorphism*

$$\mathcal{X}_q^\circ \cong (\mathcal{C}_q^\circ \times_k \mathcal{D}_q^\circ)/\mathbb{F}_q$$

where $\mathbb{F}_q$ acts diagonally.

Proof. By definition, $\mathcal{X}^\circ$ is the open subset of $\mathcal{C}\times\mathcal{D}$ where $f(x)$ and $g(y)$ are regular. Also, $\mathcal{X}_q^\circ$ is the closed subset of

$$\mathcal{X}^\circ \times_k \mathcal{Y}_q = \mathcal{C}^\circ \times_k \mathcal{D}^\circ \times_k \mathcal{Y}_q$$

with coordinates (x, y, u) where $f(x) - g(y) = \wp_q(u)$. On the other hand, $\mathcal{C}_q^\circ \times_k \mathcal{D}_q^\circ$ is isomorphic to the closed subset of

$$(\mathcal{C}^\circ \times_k \mathcal{Y}_q) \times_k (\mathcal{D}^\circ \times_k \mathcal{Y}_q) = \mathcal{C}_q^\circ \times_k \mathcal{D}_q^\circ$$

with coordinates (x, y, z, w) where $f(x) = \wp_q(z)$ and $g(y) = \wp_q(w)$.

Letting $u = z - w$, the morphism $(x, z, y, w) \mapsto (x, y, z - w)$ presents $\mathcal{C}_q^\circ \times_k \mathcal{D}_q^\circ$ as an $\mathbb{F}_q$-torsor over $\mathcal{X}_q^\circ$. □

Proof of Theorem 3.1.2. By Proposition 3.1.3, there is a rational dominant map $\mathcal{C}_q \times \mathcal{D}_q \dashrightarrow \mathcal{X}_q$ given by

$$(x, z, y, w) \mapsto (x, y, z - w).$$

This proves that $\mathcal{X}_q$ is dominated by a product of curves. Also, $\mathcal{X}_q$ is geometrically irreducible since $\mathcal{C}_q$ and $\mathcal{D}_q$ are geometrically irreducible. This proves that X_q remains irreducible over $\overline{k}(u)$. Part (3) is a consequence of part (1) and Tate's theorem on endomorphisms of abelian varieties over finite fields. See, for example, [Ulm14b, 8.2.2, 6.1.2, and 6.3.1]. The claims for $\mathcal{X}$ and X follow similarly from the fact that $\mathcal{X}$ is birational to $\mathcal{C} \times_k \mathcal{D}$. □

Using [Ulm14b, 8.2.1 and 6.3.1], we see that if X is a curve over a function field F and the BSD conjecture holds for X over a finite extension K, then it also holds over any subextension $F \subset K' \subset K$. The following is thus immediate from Theorem 3.1.2 and Lemma 8.2.2.

Corollary 3.1.4. *Let X be a smooth projective irreducible curve over $K = k(u)$ and assume that there are rational functions $f(x) \in k(x)$ and $g(y) \in k(y)$ and a separable additive polynomial $A(u) \in k[u]$ such that X is birational to the curve*

$$\{f(x) - g(y) - A(u) = 0\} \subset \mathbb{P}^1_K \times_K \mathbb{P}^1_K.$$

Then the BSD conjecture holds for the Jacobian of X.

We note that an argument similar to [Ulm14a, Rem. 12.2] shows that the hypothesis that A is separable is not needed.

To determine the genus of X_q and for later use, we now proceed to construct a specific blow-up $\phi_1 : \mathcal{X} \to \mathcal{C} \times_k \mathcal{D}$ which resolves the indeterminacy of the rational map $\psi_1 : \mathcal{C} \times_k \mathcal{D} \dashrightarrow \mathbb{P}^1_{k,t}$ and yields a morphism $\pi_1 : \mathcal{X} \to \mathbb{P}^1_{k,t}$.

Proposition 3.1.5. *The genus of the smooth proper irreducible curve X_q over K_q is*

$$g_{X_q} = Mg_{\mathcal{D}} + Ng_{\mathcal{C}} + (M-1)(N-1) - \sum_{i,j} \delta(a_i, b_j)$$

where $\delta(a,b) := (ab - a - b + \gcd(a,b))/2$.

Proof. The proof of Proposition 3.1.5 is very similar to the proof of [Ber08, Thm 3.1]; see also [Ulm13a, §4.4]. It uses facts about the arithmetic genus of curves of bidegree (M,N) in $\mathcal{C} \times_k \mathcal{D}$, the adjunction formula, and resolution of singularities.

The procedure to resolve the singularity at each base point (P_i, Q_j) is the same, so we fix one such point and drop i and j from the notation. Thus assume that (P,Q) is a base point, that f has a pole of order a at P, and that g has a pole of order b at Q. Choose uniformizers x and y at P and Q respectively, so that $f = ux^{-a}$ and $g = vy^{-b}$ where u and v are units in the local rings at P and Q respectively. The map ψ_1 is thus given in the neighborhood of (P,Q) in projective coordinates by $[uy^b - vx^a : x^a y^b]$.

The resolution of the indeterminacy at (P,Q) takes place in three stages. The first stage, which we discuss now, occurs only when $a \neq b$. Suppose that is the case and blow up the point (P,Q) on $\mathcal{C} \times_k \mathcal{D}$. Then there is a unique point of indeterminacy upstairs. If $a < b$, we introduce new coordinates $x = x_1 y_1$ and $y = y_1$ in which the blow-up composed with ψ_1 becomes $[uy_1^{b_1} - vx_1^{a_1} : x_1^{\alpha_1} y_1^{\beta_1}]$ where $a_1 = a$, $b_1 = b - a$, $\alpha_1 = a$ and $\beta_1 = b$. The unique point of indeterminacy is at $x_1 = y_1 = 0$. If $a > b$, we introduce new coordinates $x = x_1$ and $y = x_1 y_1$ in which the blow-up composed with ψ_1 becomes $[uy_1^{b_1} - vx_1^{a_1} : x_1^{\alpha_1} y_1^{\beta_1}]$ where $a_1 = a - b$, $b_1 = b$, $\alpha_1 = a$ and $\beta_1 = b$. The unique point of indeterminacy is at $x_1 = y_1 = 0$. In both cases, note that $\alpha_1 \geq a_1$ and $\beta_1 \geq b_1$.

We now proceed inductively within this case. Suppose that at step ℓ our map is given locally by $[uy_\ell^{b_\ell} - vx_\ell^{a_\ell} : x_\ell^{\alpha_\ell} y_\ell^{\beta_\ell}]$ and $a_\ell \neq b_\ell$. The point $x_\ell = y_\ell = 0$ is the point of indeterminacy. If $a_\ell < b_\ell$, we set $x_\ell = x_{\ell+1} y_{\ell+1}$ and $y_\ell = y_{\ell+1}$ so that our map becomes $[uy_{\ell+1}^{b_{\ell+1}} - vx_{\ell+1}^{a_{\ell+1}} : x_{\ell+1}^{\alpha_{\ell+1}} y_{\ell+1}^{\beta_{\ell+1}}]$ where $a_{\ell+1} = a_\ell$, $b_{\ell+1} = b_\ell - a_\ell$, $\alpha_{\ell+1} = \alpha_\ell$ and $\beta_{\ell+1} = \beta_\ell + \alpha_\ell - a_\ell$. On the other hand, if $a_\ell > b_\ell$, we set $x_\ell = x_{\ell+1}$ and $y_\ell = x_{\ell+1} y_{\ell+1}$ so that our map becomes $[uy_{\ell+1}^{b_{\ell+1}} - vx_{\ell+1}^{a_{\ell+1}} : x_{\ell+1}^{\alpha_{\ell+1}} y_{\ell+1}^{\beta_{\ell+1}}]$ where $a_{\ell+1} = a_\ell - b_\ell$, $b_{\ell+1} = b_\ell$, $\alpha_{\ell+1} = \alpha_\ell + \beta_\ell - b_\ell$ and $\beta_{\ell+1} = \beta_\ell$. (We use here that $\alpha_\ell \geq a_\ell$ and $\beta_\ell \geq b_\ell$ and we note that these inequalities continue to hold at step $\ell + 1$.)

Let $\gamma(a,b)$ be the number of steps to proceed from (a,b) to $(\gcd(a,b), 0)$ by subtracting the smaller of a or b from the larger at each step (cf. [Ulm13a, fourth paragraph of §4.4]). Then after $j = \gamma(a,b) - 1$ steps as in the preceding paragraph, our map is given by $[uy_j^{b_j} - vx_j^{a_j} : x_j^{\alpha_j} y_j^{\beta_j}]$ where $a_j = b_j = \gcd(a,b)$. To lighten notation, let us write c for $\gcd(a,b)$, α for α_j, β for β_j, x for x_j, and y for y_j, so that our map is $[uy^c - vx^c : x^\alpha y^\beta]$ and the unique point of indeterminacy in these coordinates is $x = y = 0$. Note that $\alpha, \beta \geq c$. This completes the first stage of the resolution of indeterminacy.

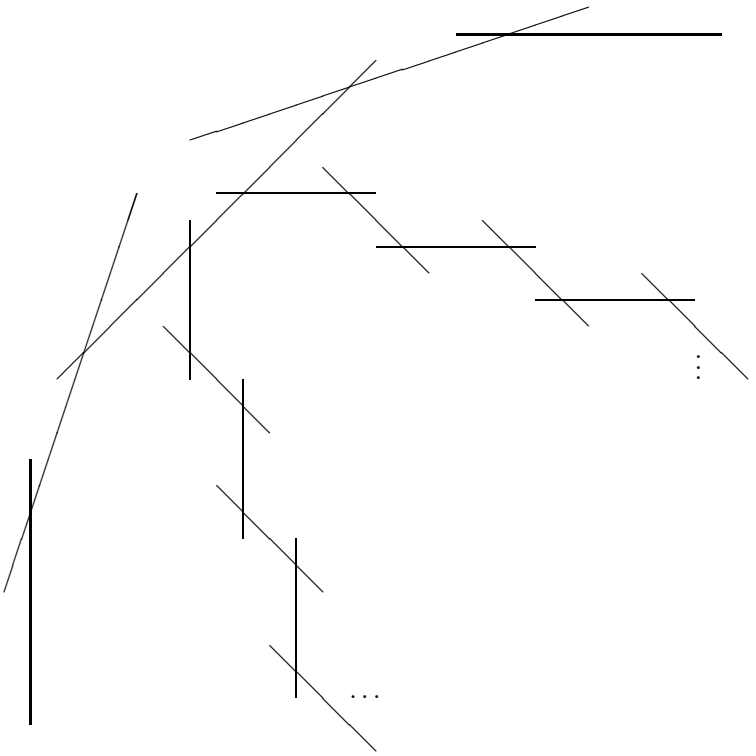

FIGURE 2. Resolution for $a = 4$, $b = 6$

The second stage consists of a single blow-up at $x = y = 0$. Introducing coordinates $x = rs$, $y = s$, our map becomes $[u - vr^c : r^\alpha s^{\beta+\alpha-c}]$, and there are now c points of indeterminacy, namely the c solutions of $r^c = u/v$, $s = 0$. (Note that $u(x) = u(rs)$ and $v(y) = v(s)$ are both constant along the exceptional divisor $s = 0$, so the equation $r^c = u/v$ has exactly c solutions on that divisor.) Let $\delta = \beta + \alpha - c$.

The third stage consists of dealing with each of the c points of indeterminacy in parallel. Focus on one of them: Replace r with $r - \omega$ where ω is one of the zeroes of $r^c - u/v$ so that our map becomes $[wr : zs^\delta]$, the point of interest is $r = s = 0$, and w and z are units in the local ring at that point. We now blow up δ times: Setting $r = r_1 s_1$, $s = s_1$, our map becomes $[wr_1 : zs_1^{\delta-1}]$; setting $r_1 = r_2 s_2$ and $s_1 = s_2$ our map is $[wr_2 : zs_2^{\delta-2}]$; ...; and after δ steps our map is $[wr_\delta; z]$ which is everywhere defined.

Figure 1 above, illustrating the case $a = 4$, $b = 6$, may help to digest the various steps. The vertical line in the lower left is the proper transform of $\mathcal{C} \times \{Q\}$, and the horizontal line in the upper right is the proper transform of $\{P\} \times \mathcal{D}$. The two lines adjacent to them are the components introduced in the first stage of the resolution, where $(a, b) = (4, 6)$ becomes $(2, 2)$ in 2 steps (so $\gamma = 3$). The line of slope 1 is the component introduced in step 2. The chains leading away from this last line are the components introduced in the third step, where $\delta = 12$ (but we have only drawn half of each chain, indicating the rest with ...).

Now we go back and consider a general element of the pencil defined by ψ and its proper transform at each stage. For all but finitely many values of t, the element of the pencil parameterized by t is smooth away from the base points. In a neighborhood of a base point (P,Q) where f and g have poles of order a and b respectively, $\mathcal{F} = \overline{\psi_1^{-1}(t)}$ is given by $uy^b - vx^a - tx^a y^b$. The tangent cone of $\mathcal{F}$ at $(0,0)$ is a single line $x = 0$ or $y = 0$, and so there is a unique point over (P,Q) on the proper transform of $\mathcal{F}$. The situation is similar for each of the first $\gamma(a,b) - 1$ blow-ups, and after the last of them, the proper transform of $\mathcal{F}$ is given locally by $uy^c - vx^c - tx^\alpha y^\beta$ in the notation at the end of the first stage above.

Now at the second stage the tangent cone consists of c lines, and there are c points over $x = y = 0$ in the proper transform. Locally the proper transform is given by $wr - zs^\delta$, and this is smooth in a neighborhood of the exceptional divisor. Therefore, there are no further changes in the isomorphism type of the proper transform in the third stage. In other words, the fibers of π_1 are isomorphic to the elements of the pencil appearing after the second stage.

To compute the genus of the fibers, we note that the multiplicity of the point of indeterminacy on $\mathcal{F}$ at the ℓ-th step of the first stage is $e_\ell = \min(a_\ell, b_\ell)$, and at the second stage it is $c = \gcd(a,b)$. Thus the change in arithmetic genus at step ℓ is $e_\ell(e_\ell - 1)/2$, and the change in the last step is $c(c-1)/2$. Summing these contributions and noting that the arithmetic genus of the elements of the original pencil is $Mg_{\mathcal{D}} + Ng_{\mathcal{C}} + (M-1)(N-1)$ yields the asserted formula for the genus g_{X_q} of the generic fiber of π_1. (See [Ber08, §§3.7 and 3.8] for more details on computing the sum.) This completes the proof. □

It is worth noting that the algorithm presented above for resolving the indeterminacy of ψ_1 sometimes leads to a morphism $\mathcal{X} \to \mathbb{P}^1_{k,t}$ which is not relatively minimal. In general, one needs to contract several (-1)-curves to arrive at a relatively minimal morphism.

Remark 3.1.6. For later use we note that the exceptional divisor of the last blow-up in stage three (at each of $c = \gcd(a,b)$ points) maps isomorphically onto the base $\mathbb{P}^1_{k,t}$, whereas all the other exceptional divisors introduced in the resolution map to the point $\infty = [1,0] \in \mathbb{P}^1_{k,t}$. In particular, $\pi_1 : \mathcal{X} \to \mathbb{P}^1_{k,t}$ always has a section, and X always has a $k(t)$-rational point.

4. Examples—lower bounds on ranks

Our goal in this section is to combine the construction of Theorem 3.1.2 with the analytic ranks bound in Corollary 2.7.3 to give examples of Jacobians which satisfy the BSD conjecture and which have large Mordell-Weil rank. This is an analogue for Artin-Schreier extensions of some results in [Ulm07] for Kummer extensions.

4.1. **Notation.** Throughout this section, k is a finite field of cardinality r, a power of p. Given an integer M and a partition $M = a_1 + \cdots + a_m$, we say that a rational function f on $\mathbb{P}^1$ is *of type* $(a_1 + \cdots + a_m)$ if the polar divisor has multiplicities $a_1, \ldots, a_m$, i.e.,

$$\operatorname{div}_\infty(f) = \sum_{i=1}^{m} a_i P_i$$

where the P_i are distinct $\overline{k}$-valued points. We assume throughout that $p \nmid a_1 \cdots a_m$. Given two non-constant rational functions f on $\mathcal{C}$ and g on $\mathcal{D}$ over k, Proposition 3.1.5 gives a formula for the genus of the smooth proper curve over $k(t)$ with equation $f - g = t$ in terms of the types of f and g.

4.2. **Elliptic curves.** Suppose now that $\mathcal{C} = \mathcal{D} = \mathbb{P}^1$ over k and that f and g are rational functions on $\mathbb{P}^1$. Straightforward calculation reveals that if the types f and g are on the following list, then the curve X over $k(t)$ given by $f(x) - g(y) = t$ has genus 1:

$$(2, 1+1), (1+1, 1+1), (2,3), (2, 2+1), (2,4), (2, 2+2), (3,3).$$

(We omit pairs of types obtained from these by exchanging the two partitions and assume $p \neq 2, 3$ as necessary.)

For example, to illustrate the $(2, 1+1)$ case, let $f(x)$ be a quadratic polynomial so that f has type (2). Let $g_1(y)$ and $g_2(y)$ be polynomials with $\deg g_1 \leq 2$ and $\deg g_2 = 2$ such that g_2 has distinct roots and g_1 and g_2 are relatively prime in $k[y]$, so that $g = g_1/g_2$ has type $(1+1)$. For such a choice of f and g, the curve $f(x) - g(y) = t$ has genus 1.

4.3. **Elliptic curves of high rank.** Recall that $K = k(t)$, q is a power of p, and $K_q = k(u)$ with $u^q - u = t$. The next result says that for certain types as in the previous section and "generic" f and g, the elliptic curve X has unbounded rank over K_q as q varies.

Proposition 4.3.1. *Suppose that $p > 2$ and f and g are rational functions on $\mathbb{P}^1$ over k of type $(2, 2+1)$ or of type $(2,4)$. Suppose that the finite critical values of g are distinct. Then the curve X defined by $f(x) - g(y) = t$ is elliptic, it satisfies the BSD conjecture over K_q for all q, and the rank of $X(K_q)$ is unbounded as q varies. More precisely, if q has the form $q = r^{2\nu}$ and k' is the field of $r^{2\nu}$ elements, then*

$$\operatorname{Rank} X(K_q) \geq \frac{r^\nu - 1}{2\nu}$$

and

$$\operatorname{Rank} X(k'K_q) \geq r^\nu - 1.$$

Proof. Proposition 3.1.5 shows that X has genus 1, and Remark 3.1.6 shows that X has a $k(t)$-rational point, so X is elliptic.

By the Riemann-Hurwitz formula, a rational function of degree M has $2M - 2$ critical points (counting multiplicities). A pole of order a is a critical point of multiplicity $a - 1$. Thus a rational function f of type (2) has 1 critical point which is not a pole, and therefore 1 finite critical value. A rational function g of type $(2+1)$ has 3 non-polar critical points, and so 3 finite critical values. Similarly, a rational function of type (4) has 3 non-polar critical points and 3 finite critical values. By "generic" we mean that the finite critical values of g are distinct, and we impose no restriction on f.

Now consider the rational map $\psi_1 : \mathcal{C} \times_k \mathcal{D} \dashrightarrow \mathbb{P}^1_{k,t}$ given by $t = f(x) - g(y)$ and the blow-up $\phi_1 : \mathcal{X} \to \mathcal{C} \times \mathcal{D}$ constructed in the proof of Proposition 3.1.5 that resolves the indeterminacy of ψ_1, yielding a proper morphism $\pi_1 : \mathcal{X} \to \mathbb{P}^1_{k,t}$ whose generic fiber is X. Away from the fiber over $t = \infty$, the critical points of π_1 are precisely the simultaneous critical points of f and g. Under our hypotheses, these are simple critical points, and so the critical points of π_1 away from the fiber

at infinity are ordinary double points. Moreover, by the counts in the previous paragraph, there are precisely three such ordinary double points. This shows that X has multiplicative reduction over three finite places of the t-line, and good reduction at all other finite places. Thus the degree of the finite part of the conductor of X is 3.

Next we claim that X (or rather the representation $H^1(X \times \overline{K}, \mathbb{Q}_\ell)$ for any $\ell \neq p$) is tamely ramified at $t = \infty$. One way to see this is to use the algorithm in the proof of Proposition 3.1.5 to compute the reduction type of X at $t = \infty$. One finds that X has Kodaira type I_3^* in the $(2, 2+1)$ case and Kodaira type III^* in the $(2, 4)$ case. In both cases, X is tamely ramified at $t = \infty$ for any $p > 2$. (Another possibility is to use the method of the proof of Proposition 4.4.1 below to see that X obtains good reduction over an extension of $k((t^{-1}))$ of degree 4.)

Now we may apply Corollary 2.7.3 to conclude that we have $\mathrm{ord}_{s=1} L(X/K_q, s) \geq (r^\nu - 1)/(2\nu)$ and $\mathrm{ord}_{s=1} L(X/k'K_q, s) \geq r^\nu - 1$. Moreover, by Theorem 3.1.2, X satisfies the BSD conjecture, so we also have a lower bound on the algebraic ranks, i.e., on $\mathrm{Rank}\, X(K_q)$ and $\mathrm{Rank}\, X(k'K_q)$.

This completes the proof of the proposition. □

The curves in Proposition 4.3.1 can of course be made quite explicit. Let us consider the case of types $(2, 2+1)$. Since f and g have unique double poles, these occur at rational points, and we may assume they are both at infinity. Thus $f(x)$ is a quadratic polynomial which, after a change of coordinates on x and t, we may take to be x^2, and g has the form

$$g(y) = \frac{ay^3 + by^2 + cy + d}{y}$$

for scalars a, b, c, d. A small calculation reveals that X has the Weierstrass form

$$y^2 = x^3 + (t + c)x^2 + bdx + ad^2.$$

The discriminant of this model is a cubic polynomial in t, and the genericity condition is simply that the discriminant have distinct roots. To see that the locus where it is satisfied is not empty, we may specialize as follows: If $p > 3$, take $a = d = 1$ and $b = c = 0$ so that X is $y^2 = x^3 + tx^2 + 1$. The discriminant is then $-16(4t^3 + 27)$, which has distinct roots. If $p = 3$, take $a = b = d = 1$ and $c = 0$, in which case the discriminant is $-t^3 + t^2 - 1$, a polynomial with distinct roots in characteristic 3.

4.4. **Unbounded rank in most genera.** The main idea of the previous section generalizes easily to most genera.

We define a pair of polynomials (f, g) to be "generic" if the set of differences $f(x_i) - g(y_j)$, where x_i and y_j run through the non-polar critical points of f and g respectively, has maximum possible cardinality. In other words, we require that if $(i, j) \neq (i', j')$, then $f(x_i) - g(y_j) \neq f(x_{i'}) - g(y_{j'})$. Note that this condition imposes no constraint on a quadratic polynomial f since it has only one finite critical value.

Proposition 4.4.1. *Fix an integer $g_X > 0$ such that p does not divide $N = 2g_X + 2$. Suppose that f and g are a pair of "generic" rational functions on $\mathbb{P}^1$ (generic in the sense mentioned above) of type $(2, N)$. Then the smooth proper curve defined by $f(x) - g(y) = t$ has genus g_X, its Jacobian J_X satisfies the BSD conjecture over K_q for all q, and the rank of $J_X(K_q)$ is unbounded as q varies through powers of p.*

Proof. We may assume that the unique poles of f and g are at infinity, so that f and g are polynomials. After a further change of coordinates on x and t, we may take $f(x) = x^2$. Thus X is a hyperelliptic curve

$$x^2 = a_N y^N + a_{N-1}x^{N-1} + \cdots + a_0 + t \tag{4.4.2}$$

where $a_0, \ldots, a_N \in k$ and $a_N \neq 0$. The BSD conjecture is true for J_X by Theorem 3.1.2, and the genus of X is $g_X = (N-1)-\delta(2,N)$, as seen in Proposition 3.1.5.

Our genericity assumption is that the $N-1$ finite critical values of g are distinct. As in the proof of Proposition 4.3.1, we see that X has an ordinary, non-separating double point at $N-1$ places of $\mathbb{P}^1$, and it has good reduction at all other finite places. This shows that the degree of the finite part of the conductor of X is $N-1 = 2g_X - 1$, an odd integer.

We now claim that at $t = \infty$, X obtains good reduction over an extension of degree N. Since $p \nmid N$ by hypothesis, this implies that X is tame at $t = \infty$. To check the claim, let v satisfy $t = v^{-N}$ and change coordinates in (4.4.2) by setting $x = x_1/v$ and $y = y_1/v^{N/2}$. The resulting model of X is

$$x_1^2 = a_N y_1^N + \sum_{i=0}^{N-1} a_i y_1^i v^{N-i} + 1.$$

This curve visibly has good reduction at $v = 0$, which establishes our claim.

Now Corollary 2.7.3 applies and shows that when $q = r^{2\nu}$,

$$\operatorname{ord}_{s=1} L(J_X/K_q, s) \geq (r^\nu - 1)/(2\nu).$$

Since J_X satisfies the BSD conjecture, we get a similar lower bound on the rank, and this completes the proof of the proposition. □

As an explicit example, assume that $p \nmid (2g_X+2)(2g_X+1)$ and take $N = 2g_X+2$, $f(x) = x^2$, and $g(y) = y^N + y$, so that X is the hyperelliptic curve

$$x^2 = y^N + y + t.$$

The finite critical values of g are $\alpha(N-1)/N$ where α runs through the roots of $\alpha^{N-1} = -1/N$, and these values are distinct under our assumptions on p. Thus this pair (f, g) is generic, and we get an explicit hyperelliptic curve whose Jacobian has unbounded rank in the tower of fields K_q.

5. A rank formula

In this section, k will be a general field of characteristic p, not necessarily finite. In the main result, we will assume k is algebraically closed for convenience, but this is not essential.

5.1. **The Jacobian of X.** We write J_X for the Jacobian of the curve X over $K = k(t)$ discussed in Theorem 3.1.2. Recall that for a power q of p, we set $K_q = k(u)$ where $\wp_q(u) = u^q - u = t$. Our main goal in this section is to give a formula for the rank of the Mordell-Weil group (as defined just below) of J_X over K_q.

First we recall the K_q/k-trace of J_X, which we denote by (B_q, τ_q). By definition, (B_q, τ_q) is the final object in the category of pairs (B, τ) where B is an abelian variety over k and $\tau : B \times_k K_q \to J_X$ is a morphism of abelian varieties over K_q. See [Con06] for a modern account.

Proposition 5.1.1. *For every power q of p, the K_q/k-trace of J_X is canonically isomorphic to $J_{\mathcal{C}} \times J_{\mathcal{D}}$.*

Proof. The proof is very similar to that of [Ulm13a, Prop. 5.6], although somewhat simpler since our hypothesis that p does not divide the pole orders of f and g implies that $\mathcal{C}_q$ and $\mathcal{D}_q$ are irreducible. We omit the details. □

Definition 5.1.2. The *Mordell-Weil group* of J_X over K_q, denoted $MW(J_X/K_q)$, is defined to be

$$\frac{J_X(K_q)}{\tau_q B_q(k)}.$$

5.2. **Two numerical invariants.** Recall that we have constructed a smooth projective surface $\mathcal{X}$ equipped with a generically smooth morphism $\pi_1 : \mathcal{X} \to \mathbb{P}^1_{k,t}$ whose generic fiber is X/K. For each closed point v of $\mathbb{P}^1_{k,t}$, let f_v denote the number of irreducible components in the fiber of π_1 over v. We define

$$c_1(q) = q \sum_{v \neq \infty} (f_v - 1) \deg v$$

where the sum is over the finite closed points of $\mathbb{P}^1_{k,t}$.

Using the notation established at the beginning of Subsection 3.1, we define

$$c_2 = \left(\sum_{i=1}^{m} \sum_{j=1}^{n} \gcd(a_i, b_j) \right) - m - n + 1.$$

We can now state the main result of this section.

Theorem 5.2.1. *Assume that k is algebraically closed. Given data $\mathcal{C}$, $\mathcal{D}$, f, and g as above, consider the smooth proper model X of*

$$\{f - g - t = 0\} \subset \mathcal{C} \times_k \mathcal{D} \times_k \operatorname{Spec}(K)$$

over $K = k(t)$ as constructed above. Let J_X be the Jacobian of X. Recall that $K_q = k(u)$ with $u^q - u = t$. Then, with $c_1(q)$ and c_2 as defined above, we have

$$\operatorname{Rank} \mathrm{MW}(J_X/K_q) = \operatorname{Rank} \operatorname{Hom}_{k-av}(J_{\mathcal{C}_q}, J_{\mathcal{D}_q})^{\mathbb{F}_q} - c_1(q) + c_2.$$

Here $\operatorname{Hom}_{k-av}$ *denotes homomorphisms of abelian varieties over k, and the exponent $\mathbb{F}_q$ signifies those homomorphisms which commute with the $\mathbb{F}_q$ actions on $J_{\mathcal{C}_q}$ and $J_{\mathcal{D}_q}$.*

Remark 5.2.2. The theorem also holds for X/K: We have $\operatorname{Rank} \mathrm{MW}(J_X/K) = \operatorname{Rank} \operatorname{Hom}_{k-av}(J_{\mathcal{C}}, J_{\mathcal{D}}) - c_1(1) + c_2$. The proof is a minor variation of what follows, but we omit it to avoid notational complications.

Proof. The proof is very similar to that of [Ulm13a, Thm. 6.4]: we will construct a good model $\pi_q : \mathcal{X}_q \to \mathbb{P}^1_{k,u}$ of X/K_q and use the Shioda-Tate formula.

First consider the rational map $\psi_q : \mathcal{C}_q \times_k \mathcal{D}_q \dashrightarrow \mathbb{P}^1_{k,u}$ defined by the formula $u = z - w$. For each pair (i, j) with $1 \leq i \leq m$, $1 \leq j \leq n$, there is a unique point $(\tilde{P}_i, \tilde{Q}_j) \in \mathcal{C}_q \times_k \mathcal{D}_q$ over $(P_i, Q_j) \in \mathcal{C} \times_k \mathcal{D}$. The indeterminacy locus of ψ_q is $\{(\tilde{P}_i, \tilde{Q}_j)\}$. At each of these base points, the blow-ups required to resolve the indeterminacy of ψ_q are identical to those described in the proof of Proposition 3.1.5 (resolving the indeterminacy of ψ_1 at (P_i, Q_j)). For each (i, j), write the total number of blow-ups over $\{(\tilde{P}_i, \tilde{Q}_j)\}$ as $N_{ij} + \gcd(a_i, b_j)$ and recall that N_{ij} of the

exceptional divisors map to $\infty \in \mathbb{P}^1$, whereas $\gcd(a_i, b_j)$ of them map isomorphically onto $\mathbb{P}^1_{k,u}$. Let $\widetilde{\mathcal{C}_q \times_k \mathcal{D}_q}$ denote this blow-up of $\mathcal{C}_q \times_k \mathcal{D}_q$.

The action of $\mathbb{F}_q^2$ on $\mathcal{C}_q \times_k \mathcal{D}_q$ lifts canonically to $\widetilde{\mathcal{C}_q \times_k \mathcal{D}_q}$. In fact, it is clear that the action of $\mathbb{F}_q^2$ on the tangent space at $\{(\tilde{P}_i, \tilde{Q}_j)\}$ is trivial, so every point in the exceptional divisor is fixed and these are the only fixed points. Therefore the quotient $\mathcal{X}_q := \widetilde{\mathcal{C}_q \times_k \mathcal{D}_q}/\mathbb{F}_q$ (quotient by the diagonal subgroup $\mathbb{F}_q \subset \mathbb{F}_q^2$) is smooth. The resolved morphism $\widetilde{\mathcal{C}_q \times_k \mathcal{D}_q} \to \mathbb{P}^1_{k,u}$ factors through $\mathcal{X}_q$ and defines a morphism $\pi_q : \mathcal{X}_q \to \mathbb{P}^1_{k,u}$ whose generic fiber is X/K_q.

It is classical (and reviewed in [Ulm11, II.8.4]) that

$$\mathrm{NS}(\mathcal{C}_q \times_k \mathcal{D}_q) \cong \mathrm{Hom}_{k-av}(J_{\mathcal{C}_q}, J_{\mathcal{D}_q}) \oplus \mathbb{Z}^2.$$

Noting that the blow-ups are fixed by the action of $\mathbb{F}_q^2$ and taking $\mathbb{F}_q$ invariants, we find that

$$\mathrm{NS}(\mathcal{X}_q) \cong \mathrm{Hom}_{k-av}(J_{\mathcal{C}_q}, J_{\mathcal{D}_q})^{\mathbb{F}_q} \oplus \mathbb{Z}^{2+\sum_{i,j}(N_{ij}+\gcd(a_i,b_j))}$$

and so

$$\mathrm{Rank}\,\mathrm{NS}(\mathcal{X}_q) = \mathrm{Rank}\,\mathrm{Hom}_{k-av}(J_{\mathcal{C}_q}, J_{\mathcal{D}_q})^{\mathbb{F}_q} + 2 + \sum_{i,j}(N_{ij} + \gcd(a_i, b_j)). \tag{5.2.3}$$

We apply the Shioda-Tate formula [Shi99] to $\mathcal{X}_q$. It says that

$$\mathrm{Rank}\,\mathrm{NS}(\mathcal{X}_q) = \mathrm{Rank}\,MW(J_X/K_q) + 2 + \sum_u (f_{u,q} - 1). \tag{5.2.4}$$

Here the sum is over the closed points of $\mathbb{P}^1_{k,u}$, and $f_{u,q}$ denotes the number of irreducible components in the fiber over u. As we noted at the beginning of the proof of Proposition 3.1.3, the complement $\mathcal{X}_q^0$ of $\pi_q^{-1}(\infty_u)$ in $\mathcal{X}_q^0$ is the fiber product of $\wp_q : \mathbb{A}^1_{k,u} \to \mathbb{A}^1_{k,t} \subset \mathbb{P}^1_{k,t}$ and $\pi_1 : \mathcal{X} \to \mathbb{P}^1_{k,t}$. Thus

$$\sum_{u \neq \infty} (f_{u,q} - 1) = q \sum_{t \neq \infty} (f_{t,1} - 1) = c_1(q).$$

Also,

$$f_{\infty,q} = \sum_{i,j} N_{ij} + m + n.$$

Substituting these into equation (5.2.4), comparing with equation (5.2.3), and solving for $\mathrm{Rank}\,MW(J_X/K_q)$ yield the claimed equality, namely

$$\mathrm{Rank}\,\mathrm{MW}(J_X/K_q) = \mathrm{Rank}\,\mathrm{Hom}_{k-av}(J_{\mathcal{C}_q}, J_{\mathcal{D}_q})^{\mathbb{F}_q} - c_1(q) + c_2.$$

This completes the proof of the theorem. □

6. Examples—exact rank calculations

In this section, we use the rank formula of Theorem 5.2.1 and results from the Appendix to give examples of various behaviors of ranks in towers of Artin-Schreier extensions.

6.1. **Preliminaries.** Throughout this section, we let $k = \overline{\mathbb{F}}_p$ and let f and g be rational functions on $\mathcal{C} = \mathcal{D} = \mathbb{P}^1$ with poles of order prime to p. Let X be the smooth proper model of $\{f(x) - g(y) - t = 0\} \subset \mathbb{P}^1_K \times_K \mathbb{P}^1_K$ where $K = k(t)$. We noted in Subsection 4.2 above that X is an elliptic curve when f and g have various types of low degree. If either f or g is a linear fractional transformation, then Proposition 3.1.5 shows that X is rational, so its Jacobian is trivial and there is nothing to say about ranks. Also, if f and g are both quadratic and both have a double pole at some point, then X is again rational by Proposition 3.1.5. The first interesting case is thus when (f, g) has type $(2, 1 + 1)$.

6.2. **Elliptic curves with bounded ranks.** Assume that $p > 2$ and that (f, g) has type $(2, 1+1)$, i.e., that f and g are quadratic rational functions such that f has a double pole and g has two distinct poles. Up to a change of coordinates on x and t, we may assume that $f(x) = x(x-a)$ with $a \in \{0, 1\}$. Also $g(y) = (y-1)(y-b)/y$ for some parameter $b \in k^\times$. The curve X is then the curve of genus 1 with affine equation

$$x(x - a)y - (y - 1)(y - b) = ty.$$

The change of coordinates $(x, y) \to (y/x, x)$ brings X into the Weierstrass form

$$y^2 - axy = x^3 + (t - 1 - b)x^2 + bx.$$

Examining the discriminant and j-invariant of this model shows that X has I_1 reduction at two finite values of t and good reduction at all other finite places, so $c_1(r) = 0$ for all r. It follows immediately from the definition that $c_2 = 0$ as well.

Thus our rank formula says that

$$\operatorname{Rank} X(K_q) = \operatorname{Rank} \operatorname{Hom}(J_{\mathcal{C}_q}, J_{\mathcal{D}_q})^{\mathbb{F}_q}.$$

Now since f has a unique pole, by Lemma 8.1.3, $J_{\mathcal{C}_q}$ has p-rank 0 for all q. On the other hand, g has simple poles, so the same lemma shows that $J_{\mathcal{D}_q}$ is ordinary for all q. Thus $\operatorname{Hom}(J_{\mathcal{C}_q}, J_{\mathcal{D}_q}) = 0$ and we have $\operatorname{Rank} X(K_q) = 0$ for all q.

6.3. **Higher genus, bounded rank.** The idea of Subsection 6.2 extends readily to higher genus. Namely, it is possible to construct curves X of every genus such that the rank of $J_X(K_q)$ is a constant independent of q. Let f be the reciprocal of a polynomial of degree M with distinct roots, and let $g = y^N$. Then X has genus $g = (M - 1)(N - 1)$ by Proposition 3.1.5.

By Lemma 8.1.3, $J_{\mathcal{C}_q}$ is ordinary whereas $J_{\mathcal{D}_q}$ has p-rank zero. It follows that $\operatorname{Hom}(J_{\mathcal{C}_q}, J_{\mathcal{D}_q}) = 0$ and *a fortiori* $\operatorname{Hom}(J_{\mathcal{C}_q}, J_{\mathcal{D}_q})^{\mathbb{F}_q} = 0$. Since the term c_1 in the rank formula is non-positive (and goes to $-\infty$ with q if it is not identically zero), and since c_2 is a constant, we see that in fact $c_1 = 0$ and the rank of $J_X(K_q)$ is bounded (in fact constant) independently of q.

If $p > 2$, we may take $N = 2$ and M arbitrary to get examples of every genus. If $p = 2$, we may take $M = 2$ and N odd to get examples of every even genus.

When $p = 2$, a similar construction produces examples of curves with odd genus. Indeed, let $\mathcal{C}$ be an ordinary elliptic curve and let f be a function on $\mathcal{C}$ with $M \geq 2$ simple poles. Applying the Lemmas 8.1.2 and 8.1.3, we see that $\mathcal{C}_q$ is an ordinary curve of genus $M(q - 1) + 1$. If $\mathcal{D} = \mathbb{P}^1$ and $g = y^N$ with N odd, then $\mathcal{D}_q$ has p-rank 0 so $\operatorname{Hom}(J_{\mathcal{C}_q}, J_{\mathcal{D}_q}) = 0$ as before. By Proposition 3.1.5, X has genus $N + (M - 1)(N - 1)$. Taking $N = 3$ yields examples of every odd genus ≥ 5.

6.4. **Elliptic curves with unbounded ranks.** Now suppose that $f = g$ is a quadratic rational function with two distinct poles. We may choose coordinates so that $f(x) = (x-1)(x-a)/x$ and $g(y) = (y-1)(y-a)/y$ for some parameter $a \in k^\times$. The curve X is then the curve of genus 1 with affine equation

$$(x-1)(x-a)y - (y-1)(y-a)x = txy.$$

The change of coordinates

$$(x,y) \to \left(-a\frac{(x-a)^2+ty}{(x-a)y}, -a\frac{(x-a)}{y}\right)$$

brings X into the Weierstrass form

$$y^2 - txy = x^3 - 2ax^2 + a^2x.$$

Straightforward calculation with Tate's algorithm gives the reduction types of X. When $p > 2$, we find that X has reduction of type I_1 at two finite places ($t = \pm\sqrt{16a}$), reduction of type I_2 at $t = 0$, and good reduction at all other finite places. When $p = 2$, X has reduction type III and conductor exponent 3 at $t = 0$, and it has good reduction at all other finite places. (Thus, the analytic ranks result of Corollary 2.7.3 gives a non-trivial lower bound on the rank of $X(K_q)$ which we will see presently is not sharp.) In all cases it follows that $c_1(q) = q$. It is also immediate from the definition that $c_2 = 1$.

Next, we note that $\mathcal{C}_q = \mathcal{D}_q$ and so

$$\mathrm{Hom}(J_{\mathcal{C}_q}, J_{\mathcal{D}_q})^{\mathbb{F}_q} = \mathrm{End}(J_{\mathcal{C}_q})^{\mathbb{F}_q}.$$

Moreover, by Lemma 8.1.3, $\mathcal{C}_q$ is ordinary. Since $k = \overline{\mathbb{F}}_p$, we know from Honda-Tate theory (cf. Lemma 8.5.2) that $\mathrm{End}(J_{\mathcal{C}_q})$ is commutative of rank $2g_{\mathcal{C}_q} = 2(q-1)$. Thus we find that

$$\mathrm{Rank}\, X(K_q) = q - 1.$$

We will study this example in much more detail in Section 7.3. In particular, we will give explicit generators of a subgroup of finite index in $X(K_q)$.

6.5. **Another elliptic curve with unbounded ranks.** In this example we take $p \neq 3$ and $f = g = x^3$. Then X is the isotrivial elliptic curve $x^3 - y^3 - t = 0$ with j-invariant 0. The change of coordinates

$$(x,y) \to \left(\frac{y+9t}{3x}, \frac{y}{3x}\right)$$

brings X into Weierstrass form

$$y^2 + 9ty = x^3 - 27t^2.$$

Tate's algorithm shows that X has good reduction away from 0 and ∞, and reduction type IV at 0. (In particular, the analytic ranks result of Corollary 2.7.3 does not give a non-trivial lower bound on the rank.) It follows that $c_1(q) = 2q$ and $c_2 = 2$. The rank formula shows that $\mathrm{Rank}\, X(K_q) = \mathrm{Rank}\, \mathrm{End}(J_{\mathcal{C}_q})^{\mathbb{F}_q} - 2(q-1)$.

Suppose that $p \equiv 2 \pmod 3$. Then the curve $\mathcal{C}_q$ is supersingular of genus $q-1$ (in other words, its Newton polygon has all slopes equal to $1/2$). Applying Lemma 8.5.2 part (3), we find that the rank of $\mathrm{End}(J_{\mathcal{C}_q})^{\mathbb{F}_q}$ is $4(q-1)$ and $\mathrm{Rank}\, X(K_q) = 2(q-1)$. In Subsection 7.2 below, we will write down explicit points generating a finite index subgroup of $X(K_q)$.

6.6. **Higher genus, unbounded rank.** It is clear from Lemma 8.5.2 that when we take $f = g$ in the construction of Section 3, in many cases the main term of the rank formula, namely $\operatorname{Rank}\operatorname{End}(J_{\mathcal{C}_q})^{\mathbb{F}_q}$, will go to infinity with q. If we can arrange the geometry so that c_1 is not too large, we will have unbounded ranks. In this subsection, we show that this is not difficult to do.

Before giving constructions, we record two easy lemmas about irreducibility of curves.

Lemma 6.6.1. *Suppose that $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ is a curve of bidegree (M, N) which has only ordinary double points as singularities. Suppose further that the number of double points is less than $\min(M, N)$. Then C is irreducible.*

Proof. If C is reducible, then it is the union of curves of bidegrees (i, j) and $(M - i, N - j)$ for some $(i, j) \neq (0, 0)$ and $\neq (M, N)$. The intersection number of the two components is $(M - i)j + (N - j)i$, and it is not hard to check that the minimum of this function over the allowable values of (i, j) is $\min(M, N)$. Thus if C has fewer than $\min(M, N)$ ordinary double points and no other singularities, then it cannot be reducible. □

Lemma 6.6.2. *Let L be an arbitrary field and let $f(x) = a(x)/b(x) \in L(x)$ be a rational function of degree M such that $a(x) - b(x)t$ is irreducible and separable in $\overline{L}(t)[x]$. Suppose that the Galois group G of the splitting field of $a(x) - b(x)t$ over $\overline{L}(t)$ is a 2-transitive subgroup of S_M. Then the plane curve with affine equation $f(x) - f(y) = 0$ (or rather $a(x)b(y) - a(y)b(x) = 0$) has exactly two irreducible components over $\overline{L}$.*

Proof. Consider the morphism $\pi_x : \mathbb{P}^1_{L,x} \to \mathbb{P}^1_{L,t}$ given by $x \mapsto t = f(x)$. The corresponding extension of function fields is $L(t) \hookrightarrow L(t)[x]/(a(x) - b(x)t) \cong L(x)$. Make a similar definition of π_y with y replacing x everywhere. Then the curve $f(x) - f(y) = 0$ is the fiber product of π_x and π_y. The function field (or rather total ring of fractions) of this fiber product is $\overline{L}(x) \otimes_{\overline{L}(t)} \overline{L}(y)$. By basic field theory, its set of irreducible components over $\overline{L}$ is in bijection with the set of orbits of G acting on ordered pairs of roots of $a(x) - b(x)t$ in $\overline{L(t)}$. By our hypotheses, there are exactly two of these, namely the diagonal (corresponding to the component $x = y$) and the rest. Thus $f(x) - g(y) = 0$ has exactly two components. □

We return to the construction of Section 3 and consider the case where $k = \overline{\mathbb{F}}_p$ and $f = g$. We assume that f has degree $M \geq 2$ and is generic in the following sense: if the critical values of $f : \mathbb{P}^1_x \to \mathbb{P}^1$ are $\alpha_1, \ldots, \alpha_{2M-2}$, then our assumption is that the set of differences $\alpha_i - \alpha_j$ for $i \neq j$ has maximum cardinality, namely $(2M-2)(2M-3)$. (This is slightly different from the condition that the pair (f, f) be generic in the sense of Subsection 4.4.)

Our assumption implies in particular that f has $2M - 2$ distinct critical values. Therefore, the type of f (in the sense of Subsection 4.1) is $1 + 1 + \cdots + 1$; i.e., f has M simple poles. In this case the genus of $\mathcal{C}_q$ is $(M - 1)(q - 1)$, $J_{\mathcal{C}_q}$ is ordinary by Lemma 8.1.3, and

$$\operatorname{Rank}\operatorname{End}(J_{\mathcal{C}_q})^{\mathbb{F}_q} = 2g_{\mathcal{C}_q} = 2(M - 1)(q - 1)$$

by Lemma 8.5.2.

Now let X be the curve over $k(t)$ defined by $f(x) - f(y) - t = 0$, with regular proper model $\pi : \mathcal{X} \to \mathbb{P}^1_{k,t}$. By Proposition 3.1.5, the genus of X is $(M - 1)^2$.

Arguing as in Subsection 4.4, we see that the fibers of π away from $t = 0, \infty$ are either smooth or have a single ordinary double point. By Lemma 6.6.1, they are thus irreducible. If we assume further that f has a large Galois group (in the sense of Lemma 6.6.2), then the fiber of π over $t = 0$ has two components. Thus $c_1 = 1$ and our rank formula says that

$$\operatorname{Rank} MW(J_X/K_q) = 2(M-1)(q-1) - q + c_2.$$

Since $M \geq 2$, the rank is unbounded as q varies. (The reader has no doubt already noticed that the case $M = 2$ is exactly the situation of Subsection 6.4.)

6.7. **Explicit curves of higher genus and unbounded rank.** As a complement to the preceding subsection, we give an example showing that even with fairly special choices of $f = g$, we get unbounded ranks. Namely, let us take $f = 1/(x^m - 1)$ where $m > 1$ is prime to $2p$. Then the curve X over $k(t)$ has equation

$$y^m - x^m - t(x^m - 1)(y^m - 1) = 0.$$

It is obvious that the fiber of $\mathcal{X}$ over $t = 0$ is reducible, with m components. We claim that for all other finite values of t, the fiber is irreducible. In other words, we claim that for all $a \in k^\times$, the plane curve

$$\mathcal{X}_a : \qquad y^m - x^m - a(x^m - 1)(y^m - 1) = 0$$

is irreducible. Since the only critical values of f are 0 and -1, both with multiplicity $m - 1$, the fibers away from $t \in \{0, \pm 1, \infty\}$ are smooth and thus, by Lemma 6.6.1, irreducible. The fiber over $t = -1$ is the curve

$$x^m y^m - 2x^m + 1 = 0.$$

We can see that this is irreducible by considering it as a Galois cover of $\mathbb{P}^1_{k,x}$ with Galois group μ_m. To wit, the cover is totally ramified over the regular points $x = (1/2)^{1/m}$, $y = 0$, so the curve must be irreducible. The argument at $t = 1$ is similar and we omit it.

Using the results of the preceding paragraph, we find that $c_1(q) = (m-1)q$, $c_2 = (m-1)^2$, and our rank formula yields

$$\begin{aligned} \operatorname{Rank} MW(X/K_q) &= 2(m-1)(q-1) - (m-1)q + (m-1)^2 \\ &= (q + m - 3)(m-1) \end{aligned}$$

which grows linearly with q.

6.8. **Analytic ranks and supersingular factors.** In this subsection, we show that the rank formula of Theorem 5.2.1 gives a connection between the symplectic and orthogonal versions of the analytic rank lower bounds, i.e., between Corollary 2.7.3 and Proposition 2.8.1.

Consider the situation of Proposition 4.3.1 with (f, g) generic of type $(2, 2+1)$ and p odd. We suppose that f and g are defined over a finite field k_0 of cardinality r, and we let $k = \overline{\mathbb{F}}_p$ and $K = k(t)$. We assume that q is a power of r^2 and set $K_q = \overline{\mathbb{F}}_p(u)$ with $u^q - u = t$.

The curve X given by $f - g = t$ has genus 1, and by Proposition 4.3.1 we have

$$\operatorname{Rank} X(K_q) - \operatorname{Rank} X(K) \geq \sqrt{q} - 1.$$

The proof of Proposition 4.3.1 shows that X has three finite places of bad reduction, each with a single ordinary double point. It follows from Lemma 6.6.1 that

the fibers are irreducible, so $c_1(q) = 0$. It is immediate that $c_2 = 1$, so the rank formula of Theorem 5.2.1 reads

$$\operatorname{Rank} X(\overline{\mathbb{F}}_p(u)) = \operatorname{Rank} \operatorname{Hom}_{\overline{\mathbb{F}}_p}(J_{\mathcal{C}_q}, J_{\mathcal{D}_q})^{\mathbb{F}_q} + 1.$$

The formula of Remark 5.2.2 for $\operatorname{Rank} X(K))$ shows that $\operatorname{Rank} X(K) = 1$. Considering the lower bound of the preceding paragraph, we find that

$$\operatorname{Rank} \operatorname{Hom}_{\overline{\mathbb{F}}_p}(J_{\mathcal{C}_q}, J_{\mathcal{D}_q})^{\mathbb{F}_q} \geq \sqrt{q} - 1.$$

Now the Jacobian of $\mathcal{C}_q$ is supersingular of dimension $(q-1)/2$. By Lemma 8.1.2 and Theorem 8.3.1, the Jacobian of $\mathcal{D}_q$ has dimension $3(q-1)/2$ and slopes 0,1/2, and 1, each with multiplicity $(q-1)$. The slopes suggest, but do not prove, that $J_{\mathcal{D}_q}$ has supersingular elliptic curves as isogeny factors. The ranks formula does prove this. Indeed, if e is the multiplicity of the supersingular elliptic curve in the Jacobian of $\mathcal{D}_q$, then

$$\operatorname{Rank} \operatorname{Hom}_{\overline{\mathbb{F}}_p}(J_{\mathcal{C}_q}, J_{\mathcal{D}_q})^{\mathbb{F}_q} = 4\frac{q-1}{2}e\frac{1}{q-1} = 2e.$$

Therefore $2e \geq \sqrt{q} - 1$, and we see that $J_{\mathcal{D}_q}$ has a supersingular elliptic curve as an isogeny factor with multiplicity at least $(\sqrt{q}-1)/2$. This is exactly the conclusion we would obtain by applying Proposition 2.8.1 directly to $\mathcal{D}_q$.

A similar discussion applies when we take (f, g) to have type $(2, N)$ with N even. If $p \equiv 1 \pmod{N}$, slope considerations (as in Theorem 8.3.1) suggest supersingular factors. Without this congruence on p, we know little about slopes. Still, for all $p \nmid 2N$ we get supersingular factors in $J_{\mathcal{D}_q}$ directly from Proposition 2.8.1 or indirectly via Corollary 2.7.3 and the rank formula of Theorem 5.2.1.

7. Examples—explicit points and heights

7.1. **A variant of the construction of Section 3.** There is a slight modification of the construction of Section 3 which is very useful for producing explicit points. To explain it, choose data $\mathcal{C}$, $\mathcal{D}$, f and g as usual. Assume that $f = g$ and that the covers $f : \mathcal{C} \to \mathbb{P}^1$ and $g : \mathcal{D} \to \mathbb{P}^1$ are geometrically Galois, necessarily with the same group G. For q a power of p, we have the curves $\mathcal{C}_q$ and $\mathcal{D}_q$ with equations $z^q - z = f(x)$ and $w^q - w = g(y)$ respectively. The surface $\mathcal{X}_q$ is birational to the quotient of $\mathcal{C}_q \times \mathcal{D}_q$ by the diagonal action of $\mathbb{F}_q$, and its function field is generated by x, y, and u with $u = z - w$.

Now consider the graph of Frobenius $Fr_q : \mathcal{C}_q \to \mathcal{D}_q$, i.e., the set

$$\{(x, z, y, w) = (x, z, x^q, z^q)\} \subset \mathcal{C}_q \times \mathcal{D}_q.$$

Its image in $\mathcal{X}_q$ is $\{(x, y, u) = (x, x^q, z - z^q) = (x, x^q, -f(x)\}$, which is obviously a multisection of $\mathcal{X}_q \to \mathbb{P}^1_u$ whose degree over $\mathbb{P}^1_u$ is equal to the degree of f. It is more convenient to have a section, and we can arrange for this by dividing $\mathcal{X}_q$ by the action induced by the diagonal or anti-diagonal action of G on $\mathcal{C}_q \times \mathcal{D}_q$. (The two quotients can be different; they can even give rise to curves X with different genera, and which to take is dictated by the circumstances at hand.) Calling (a nice model of) the quotient $\mathcal{X}'_q$, and writing X'/K_q for the generic fiber of $\mathcal{X}'_q \to \mathbb{P}^1_u$, the image of the graph of Frobenius in $\mathcal{X}'_q$ will then be a section and will give rise to a K_q-rational point of X'. We will use this variant in the two examples that follow.

7.2. **An isotrivial elliptic curve with explicit points.** For this example, we assume that $q \equiv 2 \pmod 3$, and we take $f = g = x^3$. The curve X thus has equation $x^3 - y^3 = t$. We take the quotient by $G = \mu_3$ acting anti-diagonally (i.e., $(x, y) \mapsto (\zeta x, \zeta^{-1} y)$). The invariants are generated by $X = xy$ and $Y = -x^3$, and the relation between them is $Y^2 + tY = X^3$. This is the equation of our curve X'. Note that X' and X are 3-isogenous elliptic curves, so they have the same Mordell-Weil rank, and the prime-to-3 parts of their Tate-Shafarevich groups are isomorphic. In Subsection 6.5, we found that the rank of $X(\overline{\mathbb{F}}_q(u))$ is $2(q-1)$. Presently we will find explicit points generating a subgroup of $X'(\mathbb{F}_{q^2}(u))$ of this rank.

To ease notation, we write E for X'. Note that E is isotrivial, with j-invariant $j = 0$. It becomes isomorphic to a constant curve E_0 over $\mathbb{F}_p(t^{1/3})$. The underlying E_0 is supersingular since we have assumed that $p \equiv 2 \pmod 3$.

Thus our aim is to find points on

$$E: \qquad Y^2 + tY = X^3$$

over $K = k(u)$ where $u^q - u = t$ and where k is the field of q^2 elements.

Proposition 7.2.1. *The torsion subgroup of $E(K)$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$, with non-trivial points $(0, 0)$ and $(0, -t)$.*

Proof. Let $P = (X, Y) \in E(K)$ be a non-trivial torsion point and let $L = K(v)$ where $v^3 = t$. Over L, the change of coordinates $X = v^2 x'$, $Y = v^3 y'$ gives an isomorphism between E and the constant curve $E_0 : (y')^2 + y' = (x')^3$. It is well known (see for example [Ulm11, I.6.1]) that the torsion points of $E_0(L)$ are defined over the finite constant field. Thus $(X, Y) = (av^2, bv^3)$ for some $a, b \in k$. Since these coordinates are also in K, we must have $a = 0$, and then it follows easily that $b = 0$ or $b = -1$, yielding the two points in the statement of the proposition. □

Next we construct some non-torsion points. Using the graph of Frobenius, we find a point $(X, Y) = (u^{(q+1)/3}, u)$ on $E(K)$. More precisely, the graph of Frobenius $Fr_q : \mathcal{C}_q \to \mathcal{D}_q$ is a curve in $\mathcal{C}_q \times \mathcal{D}_q$. Its image in $\mathcal{X}_q$ (which is birational to $(\mathcal{C}_q \times \mathcal{D}_q)/\mathbb{F}_q$) yields a multisection of $\mathcal{X}_q \to \mathbb{P}^1_u$ of degree 3, given by $y = x^q$ and $u = -x^3$. Taking the quotient by the action of μ_3 discussed above yields the section $X = xy = u^{(q+1)/3}$, $Y = -x^3 = u$ whose generic fiber is the desired rational point.

Now using the Galois group of $k(u)/k(t)$ and the automorphism group of E, we get $3q$ points labeled by $i \in \mathbb{Z}/3\mathbb{Z}$ and $\alpha \in \mathbb{F}_q$:

$$P_{i,\alpha} = \left(\zeta^i (u + \alpha)^{(q+1)/3}, u + \alpha\right).$$

Considering the divisor of $Y - (u+\alpha)$ shows that $\sum_{i \in (\mathbb{Z}/3\mathbb{Z})} P_{i,\alpha} = 0$. Considering the divisor of $X - Y^{(q+1)/3}\zeta^i$ shows that $\sum_{\alpha \in \mathbb{F}_q} P_{i,\alpha}$ is the 3-torsion point $(0, 0)$. Thus the subgroup of $E(K)$ generated by the $P_{i,\alpha}$ has rank at most $2(q-1)$ and contains all the torsion points of $E(K)$. We will see by calculating heights that it has rank exactly $2(q-1)$.

In the following result, we normalize away the factors of $\log r$ in the canonical height, as in [Ulm14b, Ch. 4].

Proposition 7.2.2. *The height pairing on $E(K)$ satisfies*

$$\langle P_{i,\alpha}, P_{j,\beta} \rangle = \langle P_{i-j,\alpha-\beta}, P_{0,0} \rangle.$$

We have

$$\langle P_{i,\alpha}, P_{0,0}\rangle = \begin{cases} \frac{2(q-1)}{3} & \text{if } i=0, \alpha=0, \\ -\frac{2}{3} & \text{if } i=0,\ \alpha\neq 0, \\ -\frac{q-1}{3} & \text{if } i\neq 0,\ \alpha=0, \\ \frac{1}{3} & \text{if } i\neq 0,\ \alpha\neq 0. \end{cases}$$

Proof. We refer to [Shi99] or [Ulm14b, 4.3] for a detailed account of the height pairing.

That $\langle P_{i,\alpha}, P_{j,\beta}\rangle = \langle P_{i-j,\alpha-\beta}, P_{0,0}\rangle$ follows from the fact that E is defined over $\mathbb{F}_p(t)$ and the height pairing is invariant under the action of $\mathrm{Gal}(K/\mathbb{F}_p(t))$. Thus to compute the pairing in general, we may reduce to the case where $(j,\beta)=(0,0)$. What has to be computed are intersection numbers and the components above places of K which contain the reductions of points.

We write $\mathcal{X}'\to\mathbb{P}^1_u$ for the regular minimal model of E/K and we write $P_{i,\alpha}$ also for the sections of $\mathcal{X}'$ corresponding to the points with these labels. We write O for the 0-section of $\mathcal{X}'$. With this notation, as in [CZ79, Lemma 1.18], the height is given by

$$\langle P_{i,\alpha}, P_{0,0}\rangle = -\left(P_{i,\alpha}-O\right)\cdot\left(P_{0,0}-O+D\right),$$

where the dot signifies the intersection product on $\mathcal{X}'$, and where D is a divisor with $\mathbb{Q}$-coefficients supported in fibers such that $P_{0,0}-O+D$ is orthogonal to all components of all fibers of $\mathcal{X}'\to\mathbb{P}^1$. The divisor D is easily calculated once we know which component of each fiber $P_{0,0}$ lands on; cf. [CZ79].

Standard calculations using Tate's algorithm [Tat75] show that E has reduction type IV at the places $u=\gamma\in\mathbb{F}_q$ and over $u=\infty$. The non-identity components correspond to components of the tangent cone $Y(Y+t)=0$.

The height (or degree) of $\mathcal{X}'\to\mathbb{P}^1_u$ (in the sense of [Ulm11, III.2.4]) is $(q+1)/3$, so the self-intersection of any section is $-(q+1)/3$. So, $O\cdot O = P_{0,0}\cdot P_{0,0} = -(q+1)/3$. We see that $P_{i,\alpha}\cdot O = 0$ for all (i,α) because the points $P_{i,\alpha}$ have polynomial coordinates of low degree. We briefly summarize the calculations needed to compute the multiplicity of the intersection of $P_{i,\alpha}$ and $P_{0,0}$ for $(i,\alpha)\neq(0,0)$. (i) If $\alpha=0$, then the multiplicity is $(q-2)/3$ at $u=0$ and is zero at the other finite places. (ii) If $\alpha\neq 0$, the equation for the Y coordinate shows the multiplicity is zero at every finite place. (iii) At infinity, the multiplicity is $(q+1)/3$ if $i=0$ and is $(q-2)/3$ if $i\neq 0$. Putting these local contributions together gives the "geometric part" of the height, namely $-(P_{i,\alpha}-O)\cdot(P_{0,0}-O)$.

Similar calculations show that $P_{i,\alpha}$ lands on the identity component when $\alpha\neq\gamma$ and on the non-identity component indexed by $Y=0$ at $\alpha=\gamma$ and at ∞. Thus the "correction factor" $-(P_{i,\alpha}-O)\cdot D$ is $-4/3$ if $\alpha=0$ and $-2/3$ if $\alpha\neq 0$, as in [CZ79, Lemma 1.19]. Summing the geometric part and the correction factor gives the heights asserted in the statement of the proposition. □

Let V be the subgroup of $E(K)$ generated by $\{P_{i,\alpha}\mid i\in\mathbb{Z}/3\mathbb{Z},\ \alpha\in\mathbb{F}_q\}$. It follows immediately from Proposition 7.2.2 that V has rank $2(q-1)$. Write A_n^* for the lattice of rank n dual to the A_n root lattice (cf. [CS99, 4.6.6]). It is well known to have discriminant $(n+1)^{n-1}$. For a real number a, write aA_n^* for the scaling of A_n^* by a. Then the sublattice of $E(K)/tor$ generated by the $P_{i,\alpha}$ is isomorphic to the tensor product lattice $A_2^*\otimes(\frac{1}{3}A_{q-1}^*)$. It thus has discriminant

$$R' = q^{2(q-2)}3^{1-q}.$$

Now $E(K)_{tor} = V_{tor}$ and R' is the discriminant of the lattice V/V_{tor}. The discriminant of the full lattice $E(K)/E(K)_{tor}$ is thus $R'/[E(K) : V]^2$. The integrality result of [Ulm14a, Prop. 9.1] shows that $[E(K) : V]$ divides q^{q-2}.

The degree of the L-function of E over K is $2(q-1)$. Since the rank of $E(K)$ is at least this big (by the height computation), it is equal to $2(q-1)$ and the L-function of E is $(1-q^{2(1-s)})^{2(q-1)}$. (Recall that the ground field k is the field of q^2 elements.) In particular, the leading term of the L-function at $s=1$ is 1. Using the BSD formula, we find that

$$[E(K) : V]^2 = |\text{Ш}(E/K)| q^{\frac{4}{3}(q-2)}.$$

It follows that $q^{\frac{2}{3}(q-2)}$ divides the index $[E(K) : V]$. Also by [Ulm14a, Prop. 9.1], the order of $\text{Ш}(E/K)$ is a power of p which divides $q^{\frac{2}{3}(q-2)}$.

Experience with analogous situations suggests that there should be an easily constructed subgroup of $E(K)$ whose index is $|\text{Ш}(E/K)|^{1/2}$. We now propose a candidate for this subgroup.

First, we note that since $q \equiv 2 \pmod 3$, the curve $\mathcal{C}_q$ is a quotient of the Hermitian (Fermat) curve F with equation $x_1^{q+1} = z_1^q - z_1$ via the map

$$(z_1, x_1) \mapsto (z = z_1, x = x_1^{(q+1)/3}).$$

Choose elements α, β, γ in $\overline{\mathbb{F}}_p$ satisfying $\alpha^{q^2-1} = -1$, $\gamma = \alpha^q$, and $\beta^q - \beta = \gamma^{q+1} = -\alpha^{q+1}$. Then we have an automorphism of F given by

$$(z_1, x_1) \mapsto (z_1 + \alpha x_1 + \beta, x_1 + \gamma).$$

We take the graph of this automorphism and map it to $\mathcal{C}_q \times \mathcal{D}_q$, then on to $\mathcal{X}_q$ and $\mathcal{X}_q'$, which leads to a rational point. After some simplifying algebra, we arrive at the following points:

If $p > 2$, for each solution β of $\beta^{q-1} = -1$ we have a point

$$P_\beta : \qquad (X, Y) = \left(-\left(\frac{u^2 - \beta^2}{2\beta} \right)^{(q+1)/3}, \frac{(u-\beta)^{q+1}}{2\beta} \right).$$

For each choice of β, we may act on P_β by elements of the Galois group of $k(u)/k(t)$ (sending u to $u + \alpha$ with $\alpha \in \mathbb{F}_q$) and the automorphism group of E (sending X to $\zeta_3 X$). This leads to a set of $3q(q-1)$ points, all with coordinates in $K = k(u) = \mathbb{F}_{q^2}(u)$.

If $p = 2$, it is convenient to index our points by elements $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. The corresponding point is

$$P_\beta : \qquad (X, Y) = \left(\left(\frac{(u+\beta)(u+\beta^q)}{\beta + \beta^q} \right)^{(q+1)/3}, \frac{(u+\beta)^{q+1}}{\beta + \beta^q} \right),$$

and for each value of β we can apply automorphisms of E to get a triple of points. Again we get a total of $3q(q-1)$ points.

Recall that V is the subgroup of $E(K)$ generated by the $P_{i,\alpha}$. Let V_1 be the subgroup generated by V, the P_β, and their images under the action of $\text{Gal}(K/\mathbb{F}_p(t))$ and $\text{Aut}(E)$. We conjecture that $[V_1 : V] \stackrel{?}{=} q^{\frac{2}{3}(q-2)}$ or equivalently that

$$[E(K) : V_1]^2 \stackrel{?}{=} |\text{Ш}(E/K)|.$$

For all prime powers $q \leq 32$ with $q \equiv 2 \pmod 3$, we have confirmed this conjecture by using machine calculation to compute the height pairings $\langle P_\beta, P_{i,\alpha} \rangle$.

Remark 7.2.3. If we again take $f = g = x^3$, but assume that $q \equiv 1 \pmod 3$, then we do not get any interesting results about ranks (other than what can be deduced from the above if q is a power of p with $p \equiv 2 \pmod 3$). The reason is that we have little control of the Jacobian of $\mathcal{C}_q$ in this case. It might well be ordinary, in which case we would have $\operatorname{Rank} X(\overline{\mathbb{F}}_q(u)) = 0$.

7.3. **A family of non-isotrivial elliptic curves with explicit points.** In this subsection, let $k = \mathbb{F}_q$ and suppose q is odd. Let $f(x) = (x-1)(x-a)/x$ for some $a \in k \setminus \{0, 1\}$ and let $\mathcal{X}$ be a smooth projective surface over k birational to the affine surface in $\mathbb{A}^3$ with coordinates (x, y, t) defined by

$$f(x) - f(y) = t.$$

We may choose $\mathcal{X}$ such that there is a morphism $\pi_1 : \mathcal{X} \to \mathbb{P}^1_t$ extending the projection $(x, y, t) \mapsto t$. Let $\mathcal{X}_q$ be a smooth proper model of the fiber product of π_1 and $\mathbb{P}^1_u \to \mathbb{P}^1_t$, $t = u^q - u$. The generic fiber of $\mathcal{X}_q \to \mathbb{P}^1_u$ is the curve over $k(u)$ studied in Subsection 6.4 above.

Let $\mathcal{C}_q$ and $\mathcal{D}_q$ be the smooth projective curves defined by the equations $z^q - z = f(x)$ and $w^q - w = f(y)$ respectively. We saw in the course of analyzing the construction of Section 3 that $\mathcal{X}_q$ is birational to the quotient of $\mathcal{C}_q \times_k \mathcal{D}_q$ by the diagonal action of $\mathbb{F}_q$. As in the previous section, we want to take a further quotient. Note that since f is quadratic, $\mathcal{C}_q$ and $\mathcal{D}_q$ are double covers of the z- and w-lines respectively; thus they are Galois covers with group $\mathbb{Z}/2\mathbb{Z}$. We let $\mathcal{X}'_q$ be (a smooth projective model of) the quotient of $\mathcal{X}_q$ by the diagonal action of $\mathbb{Z}/2\mathbb{Z}$.

We have a morphism $\mathcal{X}'_q \to \mathbb{P}^1_u$ sitting in a commutative diagram

$$\begin{array}{ccc} \mathcal{X}_q & \longrightarrow & \mathcal{X}'_q \\ \downarrow & & \downarrow \\ \mathbb{P}^1_u & = & \mathbb{P}^1_u \end{array}$$

We will see in a moment that the generic fiber X' of $\mathcal{X}'_q \to \mathbb{P}^1_u$ is an elliptic curve over $k(u)$ and so the morphism $X \to X'$ induced by $\mathcal{X}_q \to \mathcal{X}'_q$ is a 2-isogeny. It follows that the rank of $X'(k(u))$ is equal to the rank of $X(k(u))$, and we showed in Subsection 6.4 that this rank is $q-1$. Our main goal in this section is to exhibit an explicit set of points generating a subgroup of $X'(k(u))$ of finite index.

We now proceed to find an explicit equation for X', working birationally, i.e., with function fields. The function field of $\mathcal{X}_q$ is generated by x, y, and u, with relation $f(x) - f(y) = u^q - u$. The action of $\mathbb{Z}/2\mathbb{Z}$ sends x to a/x, y to a/y, and fixes u. Let

$$s_1 = (x + \frac{a}{x}), \qquad s_2 = (y + \frac{a}{y}), \quad \text{and} \quad s_3 = (x - \frac{a}{x})(y - \frac{a}{y}).$$

It is easy to see that the field of invariants of $\mathbb{Z}/2\mathbb{Z}$ acting on $\mathcal{X}_q$ is generated by s_1, s_3 and u. (Note that $u^q - u = t = s_1 - s_2$.) The relations are generated by

$$\begin{aligned} s_3^2 &= \left(s_1^2 - 4a\right)\left(s_2^2 - 4a\right) \\ &= \left(s_1^2 - 4a\right)\left((s_1 - t)^2 - 4a\right). \end{aligned}$$

It is thus evident that the generic fiber of $\mathcal{X}'_q \to \mathbb{P}^1_u$ is the curve X' of genus 1 with equation

$$s_3^2 = \left(s_1^2 - 4a\right)\left(s_1^2 - 2ts_1 + t^2 - 4a\right). \tag{7.3.1}$$

Now for convenience (explained below), we *assume that a is a square in k*, say $a = b^2$. Then X' has the $k(u)$-rational point $s_1 = -2b$, $s_3 = 0$. We use this point as origin and make the substitution

$$s_1 = -2b\left(\frac{X+4bt}{X-4bt}\right), \quad s_3 = \frac{4bt(4b+t)Y}{(X-4bt)^2},$$

which brings X' into the Weierstrass form

$$E: \qquad Y^2 = X(X+16b^2)(X+t^2). \tag{7.3.2}$$

(Note that E is closely related to the Legendre curve.)

We are now going to write some explicit points of $E(k(u))$. First consider the graph of the q-power Frobenius morphism $\mathcal{C}_q \to \mathcal{D}_q$, which is the closed subset $\Gamma \subset \mathcal{C}_q \times_k \mathcal{D}_q$ defined by $y = x^q$, $w = z^q$. The image of Γ in $\mathcal{X}_q$ is defined by $y = x^q$ and $u = z - z^q = -f(x)$. The image of Γ in $\mathcal{X}'_q$ is defined by

$$\begin{aligned} s_1 &= f(x) + a + 1 \\ &= -u + a + 1 \end{aligned}$$

and

$$\begin{aligned} s_3 &= \left(x - \frac{a}{x}\right)^{q+1} \\ &= \left((-u+a+1)^2 - 4a\right)^{(q+1)/2} \\ &= \left(u^2 - 2(a+1)u + (a-1)^2\right)^{(q+1)/2}. \end{aligned}$$

The image of Γ in $\mathcal{X}'_q$ turns out to be a section and yields the rational point

$$\begin{aligned} X &= 4bt\left(\frac{u^q - (b-1)^2}{u - (b+1)^2}\right), \\ Y &= \frac{4bt(4b+t)\left(u^2 - 2(a+1)u + (a-1)^2\right)^{(q+1)/2}}{\left(u-(b+1)^2\right)^2} \end{aligned}$$

on $E(k(u))$.

We write $Q(u)$ for the point in $E(k(u))$ defined by the last display. Since E is defined over $k(t)$ and the Galois group of $k(u)/k(t)$ acts via the substitutions $u \mapsto u + \alpha$, it is clear that $Q(u+\alpha)$ lies in $E(k(u))$ for all $\alpha \in \mathbb{F}_q$. To streamline coordinates, let $P(u) = Q(u + (b+1)^2)$, so that $P(u)$ is given by

$$\begin{aligned} X &= 4bt\left(\frac{u^q + 4b}{u}\right), \\ Y &= \frac{4bt(4b+t)\left(u^2 + 4bu\right)^{(q+1)/2}}{u^2}. \end{aligned}$$

For $\alpha \in \mathbb{F}_q$, write P_α for $P(u-\alpha)$.

(We note that the curve (7.3.1) has two evident rational points, namely the two points at infinity. Instead of using one of them to go to the Weierstrass form (7.3.2), we assumed that $a = b^2$ in k and used the point $s_1 = -2b$, $s_2 = 0$. This does not affect the model (7.3.2), but it does change the points $P(u)$ by translation by a torsion point. We made the choices we did because they simplify the coordinates of $P(u)$.)

Our next goal is to prove that the points P_α generate a subgroup of $E(k(u))$ of finite index. Normally we would prove a result like this using heights, but as we

will see below, the height pairings in this example are exotic, and it seems difficult to calculate the relevant determinant. Instead, we proceed using the construction of Section 5 directly.

First, we need a preliminary result on $\mathrm{End}_{k-av}(J_{\mathcal{C}_q})$. Recall from Lemma 8.5.2(2) that $\mathrm{End}^0_{k-av}(J_{\mathcal{C}_q})$ is commutative of rank $2(q-1)$ since $J_{\mathcal{C}_q}$ is ordinary of dimension $q-1$.

Lemma 7.3.3. *The subgroup of* $\mathrm{End}^0_{k-av}(J_{\mathcal{C}_q})$ *generated by the endomorphisms* $[\alpha]$ *and* $\mathrm{Fr}\circ[\alpha]$ *for* $\alpha \in \mathbb{F}_q$ *has rank* $2(q-1)$*, and thus has finite index in* $\mathrm{End}_{k-av}(J_{\mathcal{C}_q})$. (*Here* Fr *is the q-power Frobenius.*)

Proof. Lemma 8.5.2(1) implies that the subgroup of $\mathrm{End}^0_{k-av}(J_{\mathcal{C}_q})$ generated by the endomorphisms $[\alpha]$ for $\alpha \in \mathbb{F}_q$ has rank $q-1$. It is clear that $\sum_\alpha [\alpha] = 0$, so $\{[\alpha] | \alpha \in \mathbb{F}_q \setminus 0\}$ is linearly independent.

Since Fr is not a zero divisor in $\mathrm{End}^0_{k-av}(J_{\mathcal{C}_q})$, the subgroup of $\mathrm{End}^0_{k-av}(J_{\mathcal{C}_q})$ generated by the endomorphisms $\mathrm{Fr}\circ[\alpha]$ for $\alpha \in \mathbb{F}_q$ also has rank $q-1$ and $\{\mathrm{Fr}\circ[\alpha] | \alpha \in \mathbb{F}_q \setminus 0\}$ is also independent.

We will show that the two subgroups generated by

$$\{[\alpha] | \alpha \in \mathbb{F}_q \setminus 0\} \qquad \text{and} \qquad \{\mathrm{Fr}\circ[\alpha] | \alpha \in \mathbb{F}_q \setminus 0\}$$

are independent. To that end, we consider the (effective) action of $\mathrm{End}^0_{k-av}(J_{\mathcal{C}_q})$ on $H^1(J_{\mathcal{C}_q}, \overline{\mathbb{Q}}_\ell) = H^1(\mathcal{C}_q, \overline{\mathbb{Q}}_\ell)$. Computing the latter using the Leray spectral sequence for the finite map $\mathcal{C}_q \to \mathbb{P}^1_x$ and decomposing for the action of $\mathbb{F}_q$, we find that

$$H^1(\mathcal{C}_q, \overline{\mathbb{Q}}_\ell) \cong \bigoplus_{\beta \in \mathbb{F}_q} W_\beta$$

where W_β is the subspace of $H^1(\mathcal{C}_q, \overline{\mathbb{Q}}_\ell)$ where $\mathbb{F}_q$ acts via the character $\alpha \mapsto \psi_0(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha\beta))$. (Here ψ_0 is a fixed character $\mathbb{F}_p \to \overline{\mathbb{Q}}_\ell{}^\times$.) Using the Grothendieck-Ogg-Shafarevich formula, we see that each W_β with $\beta \neq 0$ has dimension 2 and $W_0 = \{0\}$. Using an exponential sum expression for the action of Fr on W_β, we see that for $\beta \neq 0$, Fr has two distinct eigenvalues on W_β: one a p-adic unit, the other a non-unit.

Now suppose that we have a linear dependence, i.e., that there are integers a_α and b_α such that

$$\sum_{\alpha \in \mathbb{F}_q{}^\times} a_\alpha [\alpha] + b_\alpha [\alpha] \circ \mathrm{Fr} = 0$$

in $\mathrm{End}^0_{k-av}(J_{\mathcal{C}_q})$. Then as endomorphisms of $H^1(\mathcal{C}_q, \overline{\mathbb{Q}}_\ell)$, we have

$$\sum_{\alpha \in \mathbb{F}_q{}^\times} a_\alpha [\alpha] = - \sum_{\alpha \in \mathbb{F}_q{}^\times} b_\alpha [\alpha] \circ \mathrm{Fr}\,.$$

Suppose that the left hand side is not zero. Then there is a β such that the left hand side is not 0 on W_β. But the left hand side acts as a (non-zero) scalar on W_β (namely $\sum_\alpha a_\alpha \psi_0(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha\beta))$). On the other hand, the right hand side acts as a (non-zero) scalar composed with Frobenius, and thus has two distinct eigenvalues. This is a contradiction, and so we must have

$$\sum_{\alpha \in \mathbb{F}_q{}^\times} a_\alpha [\alpha] = \sum_{\alpha \in \mathbb{F}_q{}^\times} b_\alpha [\alpha] \circ \mathrm{Fr} = 0.$$

It then follows from Lemma 8.5.2(1) that $a_\alpha = b_\alpha = 0$ for all α. This completes the proof of the lemma. □

We now return to the curve E.

Theorem 7.3.4. *The points $P_\alpha \in E(k(u))$ generate a subgroup of rank $q-1$ and of finite index in $E(k(u))$. The relation among them is that $\sum_{\alpha\in\mathbb{F}_q} P_\alpha$ is torsion.*

Proof. To see that the subgroup generated by the P_α has finite index in $E(K_q)$, we consider in more detail the geometry of the construction of Section 5. We have $\mathcal{C}_q \times \mathcal{D}_q$ with its action of $\mathbb{F}_q^2$, its blow-up $\mathcal{S}$, and the quotient $\mathcal{S}/\mathbb{F}_q$ by the diagonal $\mathbb{F}_q$. The resulting $\mathcal{X}_q = \mathcal{S}/\mathbb{F}_q$ is equipped with a morphism π_q to $\mathbb{P}^1_u$ whose generic fiber is $X/k(u)$. It is also equipped with an action of $\mathbb{F}_q$ (namely $\mathbb{F}_q^2$ modulo the diagonal) which induces the action of $\mathrm{Gal}(k(u)/k(t)) = \mathbb{F}_q$ on X. There is an isogeny $X \to X' \cong E$ and the P_α come from sections of π_q, so it will suffice to show that the corresponding points in $X(K_q)$ generate a subgroup of finite index.

Now the Shioda-Tate theorem tells us that the Mordell-Weil group $X(K_q)$ is a quotient of the Néron-Severi group $\mathrm{NS}(\mathcal{X}_q)$. In the course of the proof of Theorem 5.2.1 we saw that

$$\begin{aligned}\mathrm{NS}(\mathcal{X}_q) &\cong \mathrm{End}_{k-av}(J_{\mathcal{C}_q})^{\mathbb{F}_q} \oplus \mathbb{Z}^{2+\sum_{i,j}(N_{ij}+\gcd(a_i,b_j))}\\ &\cong \mathrm{End}_{k-av}(J_{\mathcal{C}_q}) \oplus \mathbb{Z}^{10}\end{aligned}$$

where the factor $\mathbb{Z}^{10}$ corresponds to the classes of the exceptional divisors of the blow-ups and the classes of (the images of) $\mathcal{C}_q \times \{pt\}$ and $\{pt\} \times \mathcal{D}_q$.

We claim that the classes in the factor $\mathbb{Z}^{10}$ all map to torsion points in $X(K_q)$. Indeed, it is clear from the discussion above that they are fixed by the action of $\mathbb{F}_q$ on $\mathcal{X}_q$. Thus they land in the $\mathbb{F}_q$-invariant part of $X(K_q)$, which is precisely $X(k(t))$, and we know the latter group has rank 0. (This claim can also be checked by straightforward, but tedious, computation.) It follows from the claim that the image of $\mathrm{End}_{k-av}(J_{\mathcal{C}_q})$ in $X(K_q)$ is a subgroup of finite index.

By Lemma 7.3.3, the subgroup of $\mathrm{End}^0_{k-av}(J_{\mathcal{C}_q})$ generated by the endomorphisms $[\alpha]$ and $\mathrm{Fr}\circ[\alpha]$ for $\alpha \in \mathbb{F}_q$ has finite index in $\mathrm{End}_{k-av}(J_{\mathcal{C}_q})$. The corresponding points in $X(K_q)$ are the images of the graphs of these endomorphisms. Moreover, it is easy to see that the graph of $[\alpha]$ maps to one component of the fiber over $u = \alpha$ (the component "$x = y$") in $\mathcal{X}_q$. Therefore, these endomorphisms map to zero in $X(K_q)$.

It follows that the image of the remaining endomorphisms $\mathrm{Fr}\circ[\alpha]$ generates a finite index subgroup of $X(K_q)$. Their images in $E(K_q)$ are precisely the points P_α, and we proved in Subsection 6.4 that $E(K_q)$ has rank $q-1$, so we have established the first claim of the theorem.

Since $\sum P_\alpha$ lies in $E(k(t))$ and we know that the rank of $E(k(t))$ is zero, the sum must be torsion. (We could also note that Lemma 8.5.2 implies that $\sum_\alpha \mathrm{Fr}\circ[\alpha]$ is trivial in $\mathrm{End}_{k-av}(J_{\mathcal{C}_q})$.)

This completes the proof of the theorem. □

Remark 7.3.5. In contrast to the situation of [Ulm14a], 2-descent is not sufficient to prove that the "visible" points P_α generate a finite index subgroup of $E(K_q)$. More precisely, when $q \neq p$, the index of the subgroup generated by the P_α in $E(K_q)$ is divisible by a large power of 2.

We turn now to a consideration of the heights of the P_α. For $\gamma \in \mathbb{F}_q$, write tr_γ for the integer defined as follows: Consider the fiber of the family (7.3.1) over $t = \gamma$. In other words, let X'_γ be the smooth projective curve given by (7.3.1) with γ substituted for t. Then tr_γ is defined by the equality

$$\#X'_\gamma(\mathbb{F}_q) = q - tr_\gamma + 1.$$

If χ denotes the non-trivial quadratic character of $\mathbb{F}_q^\times$, then we may also define tr_γ as

$$\begin{aligned} tr_\gamma &= -1 - \sum_{\beta \in \mathbb{F}_q} \chi\left(\left(\beta^2 - 4a\right)\left(\beta^2 - 2\gamma\beta + \gamma^2 - 4a\right)\right) \\ &= -1 - \sum_{\beta \in \mathbb{F}_q} \chi\left(\beta(\beta + 4b)(\beta - \gamma)(\beta - \gamma + 4b)\right). \end{aligned}$$

(The first equality comes from the standard count of points on a hyperelliptic curve as an exponential sum. The second comes from a change of variables $\beta \mapsto \beta + 2b$.)

Theorem 7.3.6. *The height pairings $\langle P_\alpha, P_\beta \rangle$ are given by*

$$\langle P_\alpha, P_\beta \rangle = \begin{cases} \frac{(3q-1)(q-1)}{4q} + \frac{1}{2} & \text{if } \alpha = \beta, \\ \frac{1-3q}{4q} + \frac{1}{4}\chi(-1) & \text{if } \alpha - \beta = \pm 4b, \\ \frac{1-3q}{4q} + \frac{1}{4} tr_{\alpha-\beta} & \text{if } \alpha - \beta \neq 0, \pm 4b. \end{cases}$$

Remarks 7.3.7.

(1) If we were to ignore the second term in each of these heights, the lattice generated by the P_α would be a scaling of the lattice A^*_{q-1}. We may view the actual lattice as a "perturbation" of A^*_{q-1} where the fluctuations are controlled by point counts on an auxiliary family of elliptic curves. This seems to us an exotic phenomenon somewhat reminiscent of mirror symmetry.

(2) The terms $1/2$ and $\frac{1}{4}\chi(-1)$ in the height formula may also be viewed as traces. To wit, we consider the "middle extension sheaf" $\mathcal{F}$ on $\mathbb{P}^1_t$ associated to the family (7.3.1). Then for $\gamma \neq 0, \pm 4b$, we have

$$tr_\gamma = \mathrm{Tr}\left(\mathrm{Fr}_q \,|\mathcal{F}_\gamma\right)$$

where $\mathcal{F}_\gamma$ is the stalk of $\mathcal{F}$ at a geometric point over $t = \gamma$. One can then show that for $\gamma = \pm 4b$ we have

$$\mathrm{Tr}\left(\mathrm{Fr}_q \,|\mathcal{F}_\gamma\right) = \chi(-1)$$

and for $\gamma = 0$ or $\gamma = \infty$ we have

$$\mathrm{Tr}\left(\mathrm{Fr}_q \,|\mathcal{F}_\gamma\right) = 1.$$

(3) As a check, we note that the Lefschetz trace formula for $\mathcal{F}$ implies that

$$\sum_{\gamma \in \mathbb{P}^1_t(\mathbb{F}_q)} \mathrm{Tr}\left(\mathrm{Fr}_q \,|\mathcal{F}_\gamma\right) = 0.$$

Thus if we interpret the $1/2$ in the formula for $\langle P_0, P_0\rangle$ as

$$\frac{1}{4}\left(\mathrm{Tr}\left(\mathrm{Fr}_q\,|\mathcal{F}_0\right) + \mathrm{Tr}\left(\mathrm{Fr}_q\,|\mathcal{F}_\infty\right)\right),$$

then we see that the sum $\sum_{\alpha\in\mathbb{F}_q} P_\alpha$ is orthogonal to all P_α; i.e., it is torsion. This is in agreement with Theorem 7.3.4.

Proof of Theorem 7.3.6. Since E is defined over $k(t)$, and the height pairing is invariant under the action of $\mathrm{Gal}(k(u)/k(t))$, we may reduce to the case where $\beta = 0$. Thus we consider $\langle P_\alpha, P_0\rangle$ and we have to compute

$$-(P_\alpha - O)\cdot(P_0 - O + D_{P_0}).$$

The height of $E/k(u)$ (in the sense of [Ulm11, III.2.4]) is equal to q, so we have $O^2 = -q$.

Next we consider $P_\alpha \cdot O$. Rewriting the coordinates of P_α slightly, we have

$$X(P_\alpha) = 4b\frac{t}{u-\alpha}\left(u-\alpha+4b\right)^q,$$
$$Y(P_\alpha) = 4b\frac{t}{u-\alpha}(4b+t)\left(u-\alpha+4b\right)^{(q+1)/2}\left(u-\alpha\right)^{(q-1)/2},$$

and since $u-\alpha$ divides t, we see that these coordinates are polynomials in u. This shows that P_α and O do not meet over any finite place of $k(u)$. Moreover, the degree in u of $X(P_\alpha)$ is $2q-1$ and the degree in u of $Y(P_\alpha)$ is $3q-1$. Since these degrees are $< 2q$ and $< 3q$ respectively, P_α and O also do not meet over $u = \infty$. Thus we have

$$P_\alpha \cdot O = P_0 \cdot O = 0.$$

Now we consider the disposition of the points at the $3q+1$ places of bad reduction, namely $u \in \mathbb{F}_q$ (so $t = 0$), $u^q - u = t = \pm 4b$, and $u = \infty$.

At the places $u \in \mathbb{F}_q$, E has multiplicative reduction of type I_4. At $u = \alpha$, $X(P_\alpha) \neq 0$, so P_α lands on the identity component. At $u = \alpha - 4b$, $X(P_\alpha)$ vanishes to high order, so P_α lands on the component labeled 2. At $u \in \mathbb{F}_q$, $u \neq \alpha, \alpha - 4b$, $X(P_\alpha)$ and $Y(P_\alpha)$ both vanish simply and so P_α lands on the component labeled either 1 or 3. Which case occurs is determined by the sign of

$$Y(P_\alpha)/X(P_\alpha) = 4b(u-\alpha)^{(q-1)/2}(u-\alpha+4b)^{-(q-1)/2} = \pm 4b.$$

We make the convention that component 1 corresponds to the case $+4b$ above. Considering components shows that if $\alpha \neq 0$, P_α and P_0 do not meet over $u = 0$, $-4b$, α, or $\alpha - 4b$. At other places with $u \in \mathbb{F}_q$, they both land on component 1 or 3 and we have to look closer for a possible intersection. Consider the X coordinate of P_α over $u = \beta$ after the blow-up at which components 1 and 3 appear. It is

$$4b\phi(\beta)(\beta - \alpha + 4b)$$

where $\phi(u) = t/(u-\alpha)(u-\beta)$ so that $\phi(\beta) = -1/(\beta-\alpha)$. The X coordinate in question is thus $4b(\beta-\alpha+4b)/(\alpha-\beta)$. The map $\alpha \mapsto 4b(\beta-\alpha+4b)/(\alpha-\beta)$ is a linear fractional transformation, thus injective, so there are no intersections between P_α and P_0 over places with $u \in \mathbb{F}_q$.

Now consider places $u = \beta$ where $u^q - u = t = 4b$. At such a place,

$$X(P_\alpha)(\beta) = 16b^2\frac{\beta-\alpha+8b}{\beta-\alpha} \neq 0.$$

Also, we have $X(P_\alpha)(\beta) = -16b^2$ if and only if $2\beta = 2\alpha - 8b$, but this is impossible since $\beta \notin \mathbb{F}_q$. This shows that P_α lands on the identity component at these places. Also, since $\alpha \mapsto (\beta - \alpha + 8b)/(\beta - \alpha)$ is injective, $X(P_\alpha) \neq X(P_{\alpha'})$ if $\alpha \neq \alpha'$; i.e., there are no points of intersection at these places.

At places $u = \beta$ where $u^q - u = t = -4b$, we have $X(P_\alpha)(\beta) = -16b^2$ and so P_α always lands on the non-identity component. A short calculation reveals that

$$X(P_\alpha) = 4b\frac{-\beta^q + \alpha}{\beta - \alpha}\left((u - \beta) - (u - \beta)^q\right).$$

After the blow-up which makes the non-identity component appear, $X(P_\alpha)$ evaluates to $4b(-\beta^q + \alpha)(\beta - \alpha)$ at $u = \beta$, and $\alpha \mapsto 4b(-\beta^q + \alpha)(\beta - \alpha)$ is injective. Thus there are no points of intersection between P_α and P_0 at the places where $t = -4b$.

Next, we consider the situation at $u = \infty$, where E has reduction of type I_{4q}. Setting $v = u^{-1}$ and changing coordinates $X = v^{-2q}X'$, $Y = v^{-3q}Y'$, the point P_α has coordinates:

$$\begin{aligned} X'(P_\alpha) &= 4b\left(v(1 - \alpha v)^{q-1} - v^q\right)\left(1 - \alpha v^q + 4b\alpha^q\right), \\ Y'(P_\alpha) &= 4b\left(v(1 - \alpha v)^{q-1} - v^q\right)\left(4bv^q + 1 - v^{q-1}\right)(1 + 4bv)^{(q+1)/2}. \end{aligned}$$

Since X' and Y' both vanish simply, P_α lands on the component labeled 1. In fact, each P_α lands on the same point on that component. (In natural coordinates this is the point $(4b, 1)$.) Moreover, by considering the next term in the Taylor expansions of X' and Y' near $v = 0$, we see that the local intersection multiplicity in $P_\alpha \cdot P_0$ is 1.

Finally, we consider possible intersections between P_α and P_0 at places where E has good reduction. At a place where the X-coordinates coincide, we would have

$$4bt\frac{u^q + 4b}{u} = 4bt\frac{u^q - \alpha + 4b}{u - \alpha}.$$

Since we have already treated the places where $t = 0$, we may assume $t \neq 0$ and then the equality above holds if and only if $u^q + 4b = u$, i.e., if and only if $t = -4b$. We already treated these places as well, so there are no further points of intersection.

Summarizing, we have shown that the "geometric" part of the height pairing is

$$-(P_\alpha - O) \cdot (P_0 - O) = \begin{cases} 2q & \text{if } \alpha = 0, \\ q - 1 & \text{if } \alpha \neq 0. \end{cases}$$

As for the "correction factor" $-D_{P_0} \cdot P_\alpha$, the local contributions at $t = 4b$ are 0, they are $1/2$ at each of the q places where $t = -4b$, and they are $(4q - 1)/4q$ at $u = \infty$.

The correction factors over $t = 0$ are more interesting. Namely, at $u - \beta$ with $\beta \neq \alpha, \alpha - 4b$, P_α lands on component ± 1 where the sign is controlled by whether or not

$$(\beta - \alpha)^{(q-1)/2}(\beta - \alpha + 4b)^{-(q-1)/2} = 1$$

i.e., by whether or not

$$(\beta - \alpha)(\beta - \alpha + 4b)$$

is a square in $\mathbb{F}_q$.

If $\alpha = 0$, then P_0 lands on the identity component at $u = 0$, on the component 2 at $u = -4b$, and on component ± 1 at other places $u = \beta$ with $\beta \in \mathbb{F}_q$. Thus the

contribution to the correction factor at places over $t = 0$ is $-(3q-2)/4$, the total correction factor is

$$-P_0 \cdot D_{P_0} = -\frac{5q^2+2q-1}{4q}$$

and the height pairing is

$$\langle P_0, P_0 \rangle = \frac{3q^2-2q+1}{4q} = \frac{(3q-1)(q-1)}{4q} + \frac{1}{2}.$$

If $\alpha = -4b$, then at $\beta = 0$ and $\beta = -4b$, one of P_0 or P_α lands on the identity component and the local contribution is zero. At $\beta = -8b$, P_0 lands on component ± 1 and P_α lands on component 2 for a local contribution of $-1/2$. At other places over $t = 0$, P_0 and P_α lie on components ± 1, and the sum of the local contributions is

$$-\sum_{\beta \neq 0, -4b, -8b} \left(\frac{1}{2} + \frac{1}{4}\chi\left(\beta(\beta+4b)(\beta+4b)(\beta+8b)\right) \right) = -\frac{q-3}{2} - \frac{1}{4}\sum_{\beta \neq 0, -4b, -8b} \chi((\beta+8b)/\beta).$$

The last sum is easily seen to be $-1-\chi(-1)$, and so the sum of the local contributions over all places over $t = 0$ is

$$-\frac{2q-5}{4} + \frac{1}{4}\chi(-1).$$

The total correction factor is

$$-P_\alpha \cdot D_{P_0} = \frac{-4q^2+q+1}{4q} + \frac{1}{4}\chi(-1),$$

and the height pairing is

$$\langle P_\alpha, P_0 \rangle = \frac{(1-3q)}{4q} + \frac{1}{4}\chi(-1).$$

The case $\alpha = 4b$ is very similar to that of $\alpha = -4b$ and we leave it as an exercise for the reader.

Now assume that $\alpha \neq 0, \pm 4b$. Then at $\beta = 0$ and $\beta = \alpha$, one of P_0 or P_α lands on the identity component and the local contribution is 0. At $\beta = -4b$ and $\beta = \alpha - 4b$, one of P_0 or P_α lands on component 2 and the other lands on component ± 1, so we get local contributions of $-1/2$. At the other $q-4$ places over $t = 0$, both P_0 and P_α land on components ± 1. The sum of the local contributions at these places is

$$-\sum_{\beta \neq 0, -4b, \alpha, \alpha-4b} \left(\frac{1}{2} + \frac{1}{4}\chi\left(\beta(\beta+4b)(\beta-\alpha)(\beta-\alpha+4b)\right) \right) = -\frac{q-4}{2} + \frac{1}{4}\left(1 + tr_\alpha\right).$$

(For the last equality, see the display just before the statement of the theorem.) Thus the sum of the local contributions at places over $t = 0$ is

$$-\frac{2q-5}{4} + \frac{1}{4}tr_\alpha,$$

the total correction factor is

$$-P_\alpha \cdot D_{P_0} = \frac{-4q^2+q+1}{4q} + \frac{1}{4}tr_\alpha,$$

and the height pairing is

$$\langle P_\alpha, P_0\rangle = \frac{(1-3q)}{4q} + \frac{1}{4}tr_\alpha.$$

This completes the proof of the theorem. □

It would be very interesting to have a conceptual explanation for the appearance of point counts in the height pairings.

8. Appendix: Auxiliary results on Artin-Schreier covers

In this section, we collect results on Artin-Schreier curves and the Newton polygons and endomorphism algebras of their Jacobians.

8.1. **The genus and p-rank of Artin-Schreier curves.** Suppose k is a perfect field of characteristic p. Suppose $\mathcal{C}$ is a smooth projective irreducible curve over k with function field $F = k(\mathcal{C})$. Let $f(x) \in F$ be a non-constant rational function. Write $\mathrm{div}_\infty(f(x)) = \sum_{i=1}^m a_i P_i$ with distinct $P_i \in \mathbb{P}^1(\overline{k})$ and all $a_i \neq 0$.

For a power q of p, let $\mathcal{C}_{q,f}$ be the smooth projective curve with function field $F[z]/(z^q - z - f)$ and let $\tau_{q,f} : \mathcal{C}_{q,f} \to \mathcal{C}$ be the morphism corresponding to the field extension $F \hookrightarrow F[z]/(z^q - z - f(x))$. We assume throughout that $\mathcal{C}_{q,f}$ is geometrically irreducible. This holds, for example, if f has a pole of order prime to p at some place of F.

Lemma 8.1.1. *If k contains $\mathbb{F}_q$, then $\tau_{q,f} : \mathcal{C}_{q,f} \to \mathcal{C}$ is a Galois cover and its Galois group G is canonically identified with $\mathbb{F}_q$.*

Proof. This is a straightforward generalization of [Sti09, 6.4.1(a-b)]. □

Lemma 8.1.2. *Let k, q, f, and $\mathcal{C}_{q,f}$ be as above. Suppose that all the poles of f have order prime to p.*

(1) *The branch locus of $\tau_{q,f}$ is $\{P_1, \dots, P_m\}$. Above each point P_i, the cover $\tau_{q,f}$ is totally ramified. If k contains $\mathbb{F}_q$ and G_i^t denotes the ramification subgroup of G at P_i in the upper numbering, then $G_i^{a_i} = G$ and G_i^t is trivial for $t > a_i$.*

(2) *The genus $g_{q,f}$ of $\mathcal{C}_{q,f}$ and the genus $g_\mathcal{C}$ of $\mathcal{C}$ are related by the formula*

$$2g_{q,f} - 2 = q(2g_\mathcal{C} - 2) + (q-1)\sum_{i=1}^m (a_i + 1).$$

In particular, if $\mathcal{C} \simeq \mathbb{P}^1$, then $g_{q,f} = \frac{1}{2}(q-1)\left(-2 + \sum_{i=1}^m (a_i+1)\right)$.

Proof. This is a straightforward generalization of [Sti09, 6.4.1(c-g)]. □

Let $\mathcal{J}_{q,f}$ be the Jacobian of $\mathcal{C}_{q,f}$ and let $\mathcal{J}_{q,f}[p]$ be its p-torsion group scheme. Recall that the *p-rank* of $\mathcal{J}_{q,f}$ is the integer s such that $\#\mathcal{J}_{q,f}[p](\overline{k}) = p^s$. The p-rank is at most the genus $g_{q,f}$ of $\mathcal{C}_{q,f}$, and $\mathcal{C}_{q,f}$ and $\mathcal{J}_{q,f}$ are said to be *ordinary* if the p-rank is maximal, i.e., $s = g_{q,f}$ [CO09, Section 1.1].

Lemma 8.1.3. *The p-rank of $\mathcal{J}_{q,f}$ is $s = 1+q(s_{\mathcal{C}}-1)+m(q-1)$. In particular, if $\mathcal{C} \simeq \mathbb{P}^1$, then $\mathcal{J}_{q,f}$ is ordinary if and only if the poles of f are all simple, and $\mathcal{J}_{q,f}$ has p-rank 0 if and only if f has exactly one pole.*

Proof. This follows from the Deuring-Shafarevich formula [Sub75, Thm. 4.2]. □

8.2. **Quotients of Artin-Schreier curves.** This section contains two results about subextensions of the Artin-Schreier extension $F \hookrightarrow F[z]/(z^q - z - f)$. The first allows us to reduce questions about the structure of the Jacobian of the curve $\mathcal{C}_{q,f}$ given by the equation $z^q - z = f$ to the case $q = p$; it is used in Subsection 8.3.

Lemma 8.2.1. *Suppose $\mathcal{C} \simeq \mathbb{P}^1$. Let S be a set of representatives for the cosets of $\mathbb{F}_p^\times \subset \mathbb{F}_q^\times$. For $\mu \in S$, let $\mathcal{Z}_\mu$ be the Artin-Schreier curve $z^p - z = \mu f$ and let $\mathcal{J}_\mu$ be the Jacobian of $\mathcal{Z}_\mu$. Then there is an isogeny*

$$\mathcal{J}_{q,f} \sim \bigoplus_{\mu \in S} \mathcal{J}_\mu.$$

Proof. By [GS91, Proposition 1.2], the set $\{Z_\mu \to \mathbb{P}^1 \mid \mu \in S\}$ is the set of degree p covers $Z \to \mathbb{P}^1$ which are quotients of $\tau : \mathcal{C}_{q,f} \to \mathbb{P}^1$. The result then follows from [KR89, Theorem C]. □

The second result is used in Section 2, where we need to work with a more general class of Artin-Schreier extensions. To that end, recall that there is a bijection between finite subgroups of $\overline{\mathbb{F}}_p$ and monic, separable, additive polynomials, i.e., polynomials of the form

$$A(x) = x^{p^\nu} + \sum_{i=0}^{\nu-1} a_i x^{p^i}$$

with $a_i \in \overline{\mathbb{F}}_p$ and $a_0 \neq 0$. The bijection identifies a subgroup H with the polynomial $A_H(x) := \prod_{\alpha \in H}(x - \alpha)$ and identifies a polynomial A with the group H_A of its roots. For example, when H is the field of order q, then $A_H(x)$ is the polynomial $\wp_q(x) = x^q - x$. For general H, note that the field generated by the coefficients of A_H is the field of p^μ elements, where p^μ is the smallest power of p such that H is stable under the p^μ-power Frobenius.

Now suppose $f \in F$ where F is the function field of a smooth projective curve defined over k. We assume that f has a pole of order prime to p at some place of F. Suppose A is a monic, separable, additive polynomial with coefficients in k. Then we have a field extension

$$K = K_{A,f} = F[x]/(A(x) - f).$$

It is geometrically Galois over F and the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_p K/\overline{\mathbb{F}}_p F)$ is canonically isomorphic to H_A. This Galois group is stable under the r-power Frobenius since A is assumed to have coefficients in k.

The next lemma is used in Section 2 to reduce questions about the field $K_{A,f}$ to the analogous questions about the field $K_{\wp_q,f}$.

Lemma 8.2.2. *Let A be a monic, separable, additive polynomial with roots in $\mathbb{F}_q$.*

1. *Then there exists a monic, separable additive polynomial B such that the composition $A \circ B$ is $\wp_q$.*
2. *Suppose $f \in F$ has a pole of order prime to p at some place of F. Suppose $A \circ B = \wp_q$. Then $K_{A,f}$ is a subfield of $K_{\wp_q,f}$ and the geometric Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_p K_{A,f}/\overline{\mathbb{F}}_p F)$ is a quotient of $\mathbb{F}_q$, namely $B(\mathbb{F}_q)$.*

Proof. Let B be the polynomial identified with the subgroup $A(\mathbb{F}_q)$. Then $B \circ A$ has degree q and kills $\mathbb{F}_q$, so must be equal to $\wp_q$. Next, we note that the set of additive polynomials with coefficients in $\mathbb{F}_q$ together with the ring structure given by addition and composition of polynomials is a (non-commutative) domain, and $\wp_q$ is in its center. (Both of these are most easily checked by noting that the ring in question is isomorphic to Drinfeld's ring of twisted polynomials $\mathbb{F}_q\{\tau\}$ where $\tau a = a^p \tau$ for $a \in \mathbb{F}_q$.) Since $B \circ A = \wp_q$, we see that $A \circ B \circ A = A \circ \wp = \wp \circ A$, and canceling yields the first claim $A \circ B = \wp_q$. The second claim follows directly from the first. □

Example 8.2.3. Assume that r is a power of an odd prime p and fix a positive integer ν. Let $A(x) = x^{r^\nu} + x$. The group H_A of roots of A generates $\mathbb{F}_q$ where $q = r^{2\nu}$. Setting $B = \wp_{r^\nu}$, we have $A \circ B = \wp_q$. If $f \in F$ has a pole of order prime to p at some place of F, then the field extension $K_{A,f}$ is a subextension of $K_{\wp_q, f}$.

8.3. **Slopes of Artin-Schreier curves.** Next we review the definition of the Newton polygon of a curve $\mathcal{C}$ of genus g defined over a finite field from [CO09, Sections 1.16, 1.18, 3,5, 3.8, 4.38, 4.49, 10.17]. The Newton polygon of $\mathcal{C}$ is the Newton polygon of (the p-divisible group of) its Jacobian $\mathcal{J}$. It is a symmetric Newton polygon of height $2g$ and dimension g; in other words, it is a lower convex polygon in $\mathbb{R}^2$, starting at $(0,0)$ and ending at $(2g, g)$, whose break points are integral such that the slopes λ are rational numbers in the interval $[0,1]$ and the slopes λ and $1-\lambda$ occur with the same multiplicity. The Newton polygon is determined by its sequence of slopes, written in ascending order, and these are the p-adic values of the zeros of the relative Frobenius morphism π_A. More precisely, if A is a simple abelian variety defined over a finite field k of cardinality r, then Tate proved that π_A generates a field which is the center of $\mathrm{End}^0(A)$ [CO09, Section 10.17]. Viewed as an algebraic number, π_A has absolute value $\sqrt{r}$ in every embedding of $\mathbb{Q}(\pi_A)$ in $\mathbb{C}$ (a Weil $\sqrt{r}$-number). The slopes of the Newton polygon of A are the p-adic valuations of π_A and the multiplicity of λ in the Newton polygon is the sum of the degrees $[\mathbb{Q}(\pi_A)_v : \mathbb{Q}_p]$ over all places v of $\mathbb{Q}(\pi_A)$ above p such that $\lambda = v(\pi_A)/v(r)$. If $\mathcal{J}$ is not simple, then its slopes are the concatenation of the slopes of its simple factors.

Next, for k a finite field of characteristic p, a power q of p, and $f \in k(x)$ a rational function with poles of order prime to p, we define a (Hodge) polygon $HP = HP(f,q)$ as follows. Write the polar divisor of f as $\mathrm{div}_\infty(f) = \sum_{i=1}^m a_i P_i$ where the a_i are all prime to p and the P_i are distinct. Define a collection of slopes by taking slopes 0 and 1 with multiplicity $(m-1)(q-1)$ and, for each pole P_i with $a_i > 1$, slopes $1/a_i, 2/a_2, \ldots, (a_i-1)/a_i$ each with multiplicity $q-1$. We have in total $2g_{\mathcal{C}_{f,q}}$ slopes, which we place in ascending order and call $s_1, \ldots, s_{2g}$. Then HP is defined to be the graph of the piecewise linear function ψ on $[0, 2g]$ with $\psi(0) = 0$ and with slope s_i on $[i-1, i]$.

Note that $NP(\mathcal{C}_{f,q})$ and $HP(f,q)$ have the same endpoints, namely $(0,0)$ and $(2g, g)$, and $NP(C_{f,q})$ lies on or over $HP(f,q)$ [Kat79]. The following is an immediate consequence of [Zhu04, Theorem 1.1 and Corollary 1.3] (which is the case $p = q$) and Lemma 8.2.1 above.

Theorem 8.3.1. *Suppose $\mathcal{C} \simeq \mathbb{P}^1$. The Newton polygon $NP(\mathcal{C}_{f,q})$ coincides with the Hodge polygon $HP(f,q)$ if and only if $p \equiv 1 \pmod{\mathrm{lcm}(a_i)}$.*

The curve $\mathcal{C}_{q,f}$ is ordinary if and only if the only slopes of its Newton polygon are 0 and 1. As an example of the theorem, note that if all poles of $f(x) \in k(x)$ are simple, then the congruence condition is empty and the Newton and Hodge polygons coincide. Moreover, the latter has only slopes 0 and 1, giving another proof that $\mathcal{C}_{f,q}$ is ordinary in this case.

8.4. **Slopes, p-ranks, and supersingular factors.** In this subsection, we collect a few remarks about slopes, p-ranks, and supersingular elliptic curves appearing in Jacobians of Artin-Schreier curves. Throughout, $\mathcal{C}_{q,f}$ is the Artin-Schreier cover of $\mathcal{C}$ determined by the equation $z^q - z = f$.

By definition, $\mathcal{C}_{q,f}$ is *supersingular* if and only if all of the slopes of its Newton polygon equal $1/2$ [CO09, Section 1.1]. If $\mathcal{C}_{q,f}$ is supersingular, then there is an isogeny $\mathcal{J}_{q,f} \otimes \overline{k} \sim \bigoplus_{i=1}^{g} E$ for a supersingular elliptic curve E [Oor74, Theorem 4.2]. As seen in [CO09, Sections 1.1 and 5.3], if $\mathcal{C}_{q,f}$ is supersingular, its Jacobian has p-rank 0, but the converse is in general false when $g_{q,f} \geq 3$.

Note that if the Jacobian of $\mathcal{C}_{q,f}$ has a supersingular elliptic curve as an isogeny factor of multiplicity e (i.e., $\mathcal{J}_{q,f} \otimes \overline{k} \sim E^e \oplus A$), then $2e$ of its slopes are $1/2$. The converse is false unless $e = g_{q,f}$; for every isogeny type other than the supersingular one, there exists an absolutely simple abelian variety having that isogeny type [LO74].

Suppose that $\operatorname{div}_\infty(f) = \sum_{i=1}^{m} a_i P_i$ where as usual the P_i are distinct $\overline{k}$-valued points of $\mathbb{P}^1$ and the a_i are prime to p. If some a_i is even, then the Hodge polygon of f has a segment of slope $1/2$. If furthermore $p \equiv 1 \pmod{\operatorname{lcm}(a_i)}$, then by Theorem 8.3.1, the Newton polygon of $\mathcal{C}_{q,f}$ also has a segment of slope $1/2$, and so it is possible that the Jacobian $\mathcal{J}_{q,f}$ of $\mathcal{C}_{q,f}$ has supersingular factors.

One case where it does follow immediately that $\mathcal{J}_{q,f}$ has supersingular factors is when p is odd and f has exactly one pole of order 2 and no other poles. Indeed, in this situation, the Newton and Hodge polygons are equal, and the latter is a segment of slope $1/2$. Since its length is $q-1$, it follows that over $\overline{k}$, $\mathcal{J}_{q,f}$ is isogenous to a supersingular elliptic curve to the power $(q-1)/2$. More generally, any Artin-Schreier curve that dominates this example will also have supersingular factors. This includes the Artin-Schreier curves $z^p - z = g(x)^2$ for any rational function $g(x)$ having poles of order prime to p.

Finally, we note that a *different* parity condition on the a_i leads to supersingular factors and therefore to slopes $1/2$. Indeed, according to Proposition 2.8.1, if $\sum(a_i+1)$ is odd and q is a power of $r^2 = |k|^2$, then $\mathcal{C}_{f,q}$ has a supersingular elliptic curve as isogeny factor with multiplicity at least $(\sqrt{q}-1)/2$. (Note that the hypothesis here implies that at least one of the a_i is even, making a connection with the previous paragraph.) This lower bound for the multiplicity of supersingular curves as isogeny factors is often not sharp, as can be seen from the main result of [vdGvdV95].

8.5. **Endomorphism algebras of Artin-Schreier curves.** The endomorphism algebras of Artin-Schreier curves are known only in special cases. We include some partial results here which are used multiple times in Sections 6 and 7. Throughout this subsection, we assume that k contains the field of q elements.

Let $\mathbb{Q}[H]$ be the group algebra of the group $H \cong \mathbb{F}_q$. By the Perlis-Walker theorem [PW50],

$$\mathbb{Q}[H] \simeq \mathbb{Q} \oplus_{a \in S} \mathbb{Q}(\zeta_p)$$

where S is a set of representatives of the cosets of $\mathbb{F}_p^* \subset \mathbb{F}_q^*$. Let W be $\overline{\mathbb{Q}}_\ell^{\,q-1}$ with $\mathbb{F}_q$ acting by the direct sum of its $q-1$ non-trivial characters.

Let $\mathcal{C}_{q,f}$ be as in the previous subsection, and let $\mathcal{J}_{q,f}$ be its Jacobian. Consider the endomorphism algebra $\mathrm{End}^0(\mathcal{J}_{q,f}) = \mathrm{End}_k(\mathcal{J}_{q,f}) \otimes \mathbb{Q}$.

If k contains the field of q elements, then $H \cong \mathbb{F}_q$ acts on $\mathcal{C}_{q,f}$. The action of H on $\mathcal{C}_{q,f}$ induces a homomorphism $\mathbb{Q}[H] \to \mathrm{End}^0(\mathcal{J}_{q,f})$. Let $\mathrm{End}^0(\mathcal{J}_{q,f})^H$ denote the subalgebra of endomorphisms which commute with the action of H, in other words, the subalgebra commuting with the image of $\mathbb{Q}[H] \to \mathrm{End}^0(\mathcal{J}_{q,f})$. We consider the composition $\mathbb{Q}[H] \to \mathrm{End}^0(\mathcal{J}_{q,f}) \subset \mathrm{End}^0(H^1(\mathcal{C}_{q,f} \times \overline{k}, \overline{\mathbb{Q}}_\ell))$, where $\ell \neq p$ is prime.

Proposition 8.5.1. *Suppose $\mathcal{C} \simeq \mathbb{P}^1$. There is a $\mathbb{Q}[H]$-module isomorphism*

$$H^1(\mathcal{C}_{q,f} \times \overline{k}, \overline{\mathbb{Q}}_\ell) \simeq W^R$$

where $R = 2g_{q,f}/(q-1) = -2 + \sum(a_i + 1)$.

Proof. Consider the representation $\rho_{q,f}$ determined by the action of H on $H^1(\mathcal{C}_{q,f} \times \overline{k}, \overline{\mathbb{Q}}_\ell)$. By the Lefschetz fixed point theorem [Mil80, V.2.8], the character $\chi(\rho_{q,f})$ satisfies

$$\chi(\rho_{q,f}) = 2\chi_{\mathrm{triv}} - 2\chi_{\mathrm{reg}} + \sum_{i=1}^{m} A_i,$$

where A_i is the character of the Artin representation attached to the branch point P_i and χ_{reg} is the character of the regular representation. By Lemma 8.1.2(2) and [Ser79, VI], for $\sigma \in \mathbb{F}_q$,

$$A_i(\sigma) = \begin{cases} -(a_i+1), & \sigma \in \mathbb{F}_q,\ \sigma \neq \mathrm{id}, \\ (a_i+1)(q-1), & \sigma = \mathrm{id}. \end{cases}$$

Thus

$$\chi(\rho_{q,f})(\sigma) = \begin{cases} 2 - \sum_{i=1}^m (a_i+1), & \sigma \neq \mathrm{id}, \\ (q-1)(-2 + \sum_{i=1}^m (a_i+1)), & \sigma = \mathrm{id}, \end{cases}$$

and therefore by Lemma 8.1.2(3),

$$\chi(\rho_{q,f})(\sigma) = \begin{cases} -R, & \sigma \neq \mathrm{id}, \\ (q-1)R, & \sigma = \mathrm{id}, \end{cases}$$

which is the character of W^R. □

Lemma 8.5.2. *Suppose that k contains the field of q elements, so that $\mathcal{C}_{f,q} \to \mathbb{P}^1$ is an $\mathbb{F}_q$-Galois extension and $H = \mathbb{F}_q$ acts on the Jacobian $\mathcal{J}_{q,f}$ of $\mathcal{C}_{q,f}$.*

1. *The image of $\mathbb{Q}[H] \to \mathrm{End}^0(\mathcal{J}_{q,f})$ has dimension $q-1$.*
2. *If $\mathcal{C}_{q,f}$ is ordinary and k is algebraic over $\mathbb{F}_p$, then $\mathrm{End}^0(\mathcal{J}_{q,f})$ is commutative of dimension $2g_{q,f}$ and so $\mathrm{End}^0(\mathcal{J}_{q,f})^H = \mathrm{End}^0(\mathcal{J}_{q,f})$ has dimension $2g_{q,f}$.*
3. *If $\mathcal{C}_{q,f}$ is supersingular and k contains the field of p^2 elements, then*

$$\mathrm{End}^0(\mathcal{J}_{q,f}) \cong M_g(D)$$

where D is the quaternion algebra ramified at p and ∞, and $\mathrm{End}^0(\mathcal{J}_{q,f})^H$ has dimension $4g_{q,f}^2/(q-1)$.

Proof.

(1) This follows from Proposition 8.5.1.
(2) See [Tat66a, Theorem 2(c)].
(3) The fact that $\mathrm{End}^0(\mathcal{J}_{q,f}) \cong M_g(D)$ can be found in [Tat66a, Theorem 2(d)]. (The assumption that $\mathbb{F}_{p^2} \subset k$ guarantees that the endomorphism algebra of a supersingular elliptic curve is D.) By part (1), the dimension of the image of $\mathbb{Q}[H] \to \mathrm{End}^0(\mathcal{J}_{q,f})$ is $q-1$. By the double centralizer theorem [Kna07, Theorem 2.43], $\mathrm{End}^0(\mathcal{J}_{q,f})^H$ has dimension $4g_{q,f}^2/(q-1)$. □

Acknowledgement

The authors would like to thank Chris Hall for useful data about L-functions of Artin-Schreier extensions and stimulating conversations about the topics in this paper. Thanks also to the referee for a critical reading of the paper. The first author was partially supported by NSF grant DMS-11-01712.

References

[Ber08] Lisa Berger, *Towers of surfaces dominated by products of curves and elliptic curves of large rank over function fields*, J. Number Theory **128** (2008), no. 12, 3013–3030, DOI 10.1016/j.jnt.2008.03.009. MR2464851 (2009k:11107)

[CO09] Ching-Li Chai and Frans Oort, *Moduli of abelian varieties and p-divisible groups*, Arithmetic geometry, Clay Math. Proc., vol. 8, Amer. Math. Soc., Providence, RI, 2009, pp. 441–536. MR2498069 (2010j:14085)

[Con06] Brian Conrad, *Chow's K/k-image and K/k-trace, and the Lang-Néron theorem*, Enseign. Math. (2) **52** (2006), no. 1-2, 37–108. MR2255529 (2007e:14068)

[CS99] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, 3rd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 290, Springer-Verlag, New York, 1999. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. MR1662447 (2000b:11077)

[CZ79] David A. Cox and Steven Zucker, *Intersection numbers of sections of elliptic surfaces*, Invent. Math. **53** (1979), no. 1, 1–44, DOI 10.1007/BF01403189. MR538682 (81i:14023)

[DD13] Tim Dokchitser and Vladimir Dokchitser, *Growth of III in towers for isogenous curves*, Compos. Math. **151** (2015), no. 11, 1981–2005, DOI 10.1112/S0010437X15007423. MR3427571

[GS91] Arnaldo García and Henning Stichtenoth, *Elementary abelian p-extensions of algebraic function fields*, Manuscripta Math. **72** (1991), no. 1, 67–79, DOI 10.1007/BF02568266. MR1107453 (92j:11139)

[Kat79] Nicholas M. Katz, *Slope filtration of F-crystals*, Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Astérisque, vol. 63, Soc. Math. France, Paris, 1979, pp. 113–163. MR563463 (81i:14014)

[Kna07] Anthony W. Knapp, *Advanced algebra*, Cornerstones, Birkhäuser Boston, Inc., Boston, MA, 2007. Along with a companion volume *Basic algebra*. MR2360434 (2009d:00001)

[KR89] E. Kani and M. Rosen, *Idempotent relations and factors of Jacobians*, Math. Ann. **284** (1989), no. 2, 307–327, DOI 10.1007/BF01442878. MR1000113 (90h:14057)

[LO74] Hendrik W. Lenstra Jr. and Frans Oort, *Simple abelian varieties having a prescribed formal isogeny type*, J. Pure Appl. Algebra **4** (1974), 47–53. MR0354686 (50 #7163)

[Mil80] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980. MR559531 (81j:14002)

[Oor74] Frans Oort, *Subvarieties of moduli spaces*, Invent. Math. **24** (1974), 95–119. MR0424813 (54 #12771)

[PW50] Sam Perlis and Gordon L. Walker, *Abelian group algebras of finite order*, Trans. Amer. Math. Soc. **68** (1950), 420–426. MR0034758 (11,638k)

[Ser70] Jean-Pierre Serre, Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures), In *Séminaire Delange-Pisot-Poitou: 1969/70, Théorie des Nombres, Fasc. 2, Exp. 19*, Secrétariat mathématique, Paris, 1970, page 12.

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. MR554237 (82e:12016)

[Shi99] Tetsuji Shioda, *Mordell-Weil lattices for higher genus fibration over a curve*, New trends in algebraic geometry (Warwick, 1996), London Math. Soc. Lecture Note Ser., vol. 264, Cambridge Univ. Press, Cambridge, 1999, pp. 359–373, DOI 10.1017/CBO9780511721540.015. MR1714831 (2000g:11053)

[Sti09] Henning Stichtenoth, *Algebraic function fields and codes*, 2nd ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009. MR2464941 (2010d:14034)

[Sub75] Doré Subrao, *The p-rank of Artin-Schreier curves*, Manuscripta Math. **16** (1975), no. 2, 169–193. MR0376693 (51 #12868)

[Tat65] John T. Tate, *Algebraic cycles and poles of zeta functions*, Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), Harper & Row, New York, 1965, pp. 93–110. MR0225778 (37 #1371)

[Tat66a] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR0206004 (34 #5829)

[Tat66b] John Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1995, pp. Exp. No. 306, 415–440. MR1610977

[Tat75] John Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., Vol. 476, Springer, Berlin, 1975, pp. 33–52. MR0393039 (52 #13850)

[Ulm07] Douglas Ulmer, *L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields*, Invent. Math. **167** (2007), no. 2, 379–408, DOI 10.1007/s00222-006-0018-x. MR2270458 (2007k:11101)

[Ulm11] Douglas Ulmer, *Elliptic curves over function fields*, Arithmetic of L-functions, IAS/Park City Math. Ser., vol. 18, Amer. Math. Soc., Providence, RI, 2011, pp. 211–280. MR2882692

[Ulm13a] Douglas Ulmer, *On Mordell-Weil groups of Jacobians over function fields*, J. Inst. Math. Jussieu **12** (2013), no. 1, 1–29, DOI 10.1017/S1474748012000618. MR3001733

[Ulm13b] Douglas Ulmer, *Conductors of ℓ-adic representations*, Proc. Amer. Math. Soc., electronically published on October 5, 2015, DOI: http://dx.doi.org/10.1090/proc/12880 (to appear in print).

[Ulm14a] Douglas Ulmer, *Explicit points on the Legendre curve*, J. Number Theory **136** (2014), 165–194, DOI 10.1016/j.jnt.2013.09.010. MR3145329

[Ulm14b] Douglas Ulmer, *Curves and Jacobians over function fields*, In G. Boeckle et al., editors, Arithmetic Geometry over Global Function Fields, Advanced Courses in Mathematics CRM Barcelona, Springer, Basel, 2014, pp. 281–337.

[vdGvdV95] Gerard van der Geer and Marcel van der Vlugt, *On the existence of supersingular curves of given genus*, J. Reine Angew. Math. **458** (1995), 53–61. MR1310953 (95k:11084)

[Zhu04] Hui June Zhu, *L-functions of exponential sums over one-dimensional affinoids: Newton over Hodge*, Int. Math. Res. Not. **30** (2004), 1529–1550, DOI 10.1155/S1073792804132698. MR2049830 (2005h:11174)

Department of Mathematics, Colorado State University, Fort Collins, Colorado 80523

E-mail address: pries@math.colostate.edu

School of Mathematics, Georgia Institute of Technology, Atlanta, Georgia 30332

E-mail address: ulmer@math.gatech.edu