THE DIEUDONNÉ MODULES AND EKEDAHL-OORT TYPES OF JACOBIANS OF HYPERELLIPTIC CURVES IN ODD CHARACTERISTIC

SANATH DEVALAPURKAR AND JOHN HALLIDAY

ABSTRACT. Given a principally polarized abelian variety A of dimension g over an algebraically closed field k of characteristic p, the p torsion $A[p]$ is a finite flat p-torsion group scheme of rank p^{2g}. There are exactly 2^g possible group schemes that can occur as some such $A[p]$. In this paper, we study which group schemes can occur as $J[p]$, where J is the Jacobian of a hyperelliptic curve defined over $\mathbb{F}_p$. We do this by computing explicit formulae for the action of Frobenius and its dual on the de Rham cohomology of a hyperelliptic curve with respect to a given basis. A theorem of Oda's in [Oda69] allows us to relate these actions to the p-torsion structure of the Jacobian. Using these formulae and the computer algebra system Magma, we affirmatively resolve questions of Glass and Pries in [Cor05] on whether certain group schemes of rank p^8 and p^{10} can occur as $J[p]$ of a hyperelliptic curve of genus 4 and 5 respectively.

1. Introduction

Let k be a field of characteristic p. Recall that an elliptic curve E over k is a 1-dimensional group variety over k. We denote the p-torsion of E as a group scheme by $E[p]$, and the p-torsion points of E over $\overline{k}$ by $E(\overline{k})[p]$. Although in characteristic 0 the p-torsion of an elliptic curve over an algebraically closed field is isomorphic to $(\mathbf{Z}/p)^2$, in characteristic p we can either have $E(\overline{k})[p] = \mathbf{Z}/p$ or $E(\overline{k})[p] = \{0\}$ as abstract groups. The former condition is called ordinary, and happens for a generic elliptic curve. The latter is called supersingular. Now considering the p-torsion as a group scheme and not merely a group of points, we have that if E is ordinary then we have $E[p] = \mathbf{Z}/p\mathbf{Z} \oplus \mu_p$ (where $\mathbf{Z}/p\mathbf{Z}$ is the p-torsion of the p- divisible group $\mathbf{Q}_p/\mathbf{Z}_p$, and μ_p is the p-torsion of the multiplicative group scheme $\mathbf{G}_m$). On the other hand, if E is a supersingular elliptic curve, the p-torsion $E[p]$ sits in a nonsplit short exact sequence

$$0 \to \alpha_p \to E[p] \to \alpha_p \to 0,$$

where $\alpha_p \simeq \operatorname{Spec} k[x]/x^p$ is the kernel of the Frobenius on the additive group $\mathbf{G}_a$.

For principally polarized abelian varieties of dimension greater than 1, this generalizes in an especially rich way. Let A be a principally polarized abelian variety over k of dimension g; this is a k-point of the moduli space $\mathscr{A}_g$ of principally polarized abelian varieties of dimension g. Since A is an abelian variety, it admits a multiplication-by-p map $[p]\colon A \to A$, which factors as the composite $V \circ F$. Here $F\colon A \to A^{(p)}$ is the relative Frobenius, and V, called the Verschiebung, is the dual of F. (There are identifications $\ker F = \operatorname{im} V$ and $\ker V = \operatorname{im} F$, owing to the principal polarization on A.) Note that we also have $[p] = F \circ V$. The p-torsion of A is denoted $A[p]$.

The morphism $[p]$ is proper and flat of degree p^{2g}, so $A[p]$ is a p-torsion group scheme of rank p^{2g}, with induced morphisms F and V. The scheme structure of $A[p]$ is interesting, especially in dimensions greater than 1.

This motivates one to consider certain invariants of $A[p]$. The *p-rank* f of A is defined to be $\dim_{\mathbf{F}_p} \operatorname{Hom}(\mu_p, A[p])$, while the *$a$-number* a of A is defined to be $\dim_k \operatorname{Hom}(\alpha_p, A[p])$. It follows that the p-rank is the integer f such that $A[p](k) \simeq (\mathbf{Z}/p\mathbf{Z})^f$, so that $p^f = \#A[p](k)$. This implies that

$$0 \leq f \leq g.$$

Moreover, it is known that

$$1 \leq a + f \leq g.$$

In analogy to the case of dimension 1, we say that A is *ordinary* if $f = g$. This implies that $a = 0$, and that $A[p] \simeq (\mathbf{Z}/p\mathbf{Z} \oplus \mu_p)^f$. Most abelian varieties are ordinary, in that the ordinary abelian varieties comprise an open subscheme of $\mathscr{A}_g$. At the opposite end, we have *superspecial* abelian varieties, which have p-rank 0 and a-number g. In this case, $A[p] = G^g$ where G sits in the nonsplit exact sequence

$$0 \to \alpha_p \to G \to \alpha_p \to 0.$$

In fact, such an abelian variety is isogenous to E^g where E is a supersingular elliptic curve, so such abelian varieties are very rare.

In general, one can get a concrete algebraic handle on $A[p]$ by describing its *Dieudonné module*. The scheme $A[p]$ is a Barsotti–Tate group scheme (also known as a BT_1 group scheme); this means that it arises as the p-torsion of a p-divisible group over k. While this is a rather large and complicated category to get a handle on, the main theorem of Dieudonné theory lets us linearize the problem.

Theorem 1.1. *There is an equivalence of categories between* BT_1 *group schemes and k-vector spaces with maps F and V such that $FV = VF = 0$,* $\operatorname{im} F = \ker V$*, and* $\operatorname{im} V = \ker F$*. This latter category is equivalent to finite (left) modules over the Cartier–Dieudonné ring*

$$\mathrm{Cart}_p \coloneqq k[F, V]/(FV = VF = 0, Fx = x^p F, V x^p = xV).$$

The *Dieudonné module* of an abelian variety A over k is the image of $A[p]$ under the equivalence of categories in Theorem 1.1; this module will be denoted $D(A)$.

In this paper, we study which $D(A)$ can occur for A the Jacobian of a hyperelliptic curve C over $\mathbf{F}_p$. To do this, we use the following theorem of Oda to reduce the question to studying the actions of F and V on the de Rham cohomology of C.

Theorem 1.2. [Oda69] *Let C be a smooth curve over k of genus g. There is an isomorphism of* Cart_p*-modules between* $D(\mathrm{Jac}(C))$ *and* $\mathrm{H}^1_{\mathrm{dR}}(C)$.

Therefore, if we can effectively compute the action of F and V on $\mathrm{H}^1_{\mathrm{dR}}(C)$, we can determine the group scheme structure of $\mathrm{Jac}(C)[p]$. One is therefore interested in the following question[1]:

Question 1. What is the action of the Frobenius (and the Verschiebung) on $\mathrm{H}^1_{\mathrm{dR}}(C)$? Equivalently, what is the Dieudonné module of the Jacobian of a hyperelliptic curve C modulo p?

As a consequence of performing this computation, we will also be able to describe the Ekedahl–Oort type (reviewed below) of Jacobians of hyperelliptic curves.

In characteristic 2, Elkin and Pries [EP13] have computed the Dieudonné module of the Jacobian of a hyperelliptic curve. We will recall their result here.

Theorem 1.3. [EP13] *Let $C \colon y^2 - y = f(x)$ be a hyperelliptic curve over k (of characteristic* 2*). Let B denotes the set of branch points of $C \to \mathbf{P}^1$, and write*

$$f(x) = \sum_{\alpha \in B} f_\alpha(x_\alpha),$$

[1] This is an approximation to a harder question of computing the action of F and V on the crystalline cohomology of C, which reduces mod p to de Rham cohomology.

where $x_\alpha = (x-\alpha)^{-1}$ *and* $f_\alpha(x) \in xk[x^2]$ *is a polynomial of certain degree with no monomials of even exponent. Let* Y_α *denote the curve* $y^2 - y = f_\alpha(x)$*. Then*

$$\mathrm{H}^1_{\mathrm{dR}}(C) \simeq D(\mathrm{Jac}(C)) \simeq (\mathbf{Z}/p\mathbf{Z} \oplus \mu_p)^{\#B-1} \oplus \bigoplus_{\alpha\in B} \mathrm{H}^1_{\mathrm{dR}}(Y_\alpha).$$

Moreover, Elkin and Pries compute the Dieudonné module structure of $\mathrm{H}^1_{\mathrm{dR}}(Y_\alpha)$ (see [EP13, Theorem 1.3]). A similar result cannot be made in such generality in odd characteristics, since we do not have Artin–Schreier properties.

The goal of this paper is to extend the above computation to odd characteristics. Let C be a hyperelliptic curve of genus g defined by an equation $y^2 = f(x) = \sum_{k=0}^{d} a_k x^k$ over a perfect field k of characteristic $p \geq 3$. One can pick an open cover $\{U, V\}$ of C, so that (by writing down a Čech resolution) elements of $\mathrm{H}^1_{\mathrm{dR}}(C)$ are expressible as (classes of) triples (ω_U, ω_V, f), where $\omega_U \in \Gamma(U, \Omega_U)$, $\omega_V \in \Gamma(V, \Omega_V)$, and $f \in \Gamma(U\cap V, \mathscr{O}_{U\cap V})$. The main technical results of this paper can be stated as follows (see §3):

Theorem A. *In the above setup, there is an explicit choice of basis for the* $2g$*-dimensional vector space* $\mathrm{H}^1_{\mathrm{dR}}(C)$*, given by*

$$\widetilde{\tau}_i = \left(x^i \frac{dx}{y}, x^i \frac{dx}{y}, 0\right),$$
$$\widetilde{\eta}_j = \left(\omega_1^{(j)}, \omega_2^{(j)}, yx^{-j}\right),$$

for $0 \leq i \leq g-1$ *and* $1 \leq j \leq g$*; here,* $\omega_1^{(j)}$ *and* $\omega_2^{(j)}$ *are differential forms defined as:*

$$\omega_1^{(j)} = \sum_{k=0}^{j} (k-2j) a_k x^{k-j-1} \frac{dx}{2y},$$
$$\omega_2^{(j)} = -\left(\sum_{j+1}^{d} (k-2j) a_k x^{k-j-1} \frac{dx}{2y}\right).$$

We also compute the matrices of Frobenius and Verschiebung:

Theorem B. *Define* c_i *to be the coefficient of* x^i *in* $f(x)^{(p-1)/2}$*. Then, we have the following.*

(1) *The matrix of Verschiebung on* $\mathrm{H}^1_{\mathrm{dR}}(C)$ *is determined by:*
- *The coefficient of* $\widetilde{\eta}_i$ *in* $V(\widetilde{\eta}_j)$ *is zero.*
- *The coefficient of* $\widetilde{\tau}_i$ *in* $V(\eta_j)$ *is*

$$\sum_{k=0}^{j} (k-2j) a_k^{1/p} c_{ip-k+j}^{1/p}.$$

- *The coefficient of* $\widetilde{\eta}_i$ *in* $V(\widetilde{\tau}_j)$ *is zero.*
- *The coefficient of* $\widetilde{\tau}_i$ *in* $V(\widetilde{\tau}_j)$ *is given by* $c_{ip-j}^{1/p}$*.*

(2) *The matrix of Frobenius on* $\mathrm{H}^1_{\mathrm{dR}}(C)$ *is determined by:*
- *The* $\widetilde{\eta}_i$ *coefficient of* $F(\widetilde{\eta}_j)$ *is* c_{pj-i}*.*
- *The* $\widetilde{\tau}_i$ *coefficient of* $F(\widetilde{\eta}_j)$ *is*

$$\sum_{k=g+1}^{d-i} (k-i) c_{pj-k} a_{k+i}.$$

- *The* $\widetilde{\eta}_i$ *coefficient of* $F(\widetilde{\tau}_j)$ *is zero.*
- *The* $\widetilde{\tau}_i$ *coefficient of* $F(\widetilde{\tau}_j)$ *is zero.*

This computation can be used to study the behavior of certain special types of hyperelliptic curves.

Theorem C. *Let d be an odd prime such that $g = \frac{d-1}{2}$ is also prime. Let p be a prime not equal to d. Then the Jacobian of the hyperelliptic curve $y^2 = x^d + 1$ is ordinary if $p \equiv 1 \pmod{d}$, and has p-rank 0 if $p \not\equiv 1 \pmod{d}$.*

We can also answer some questions posed by Glass and Pries in [Cor05] regarding the existence of certain hyperelliptic curves whose Jacobians realize a certain Dieudonné module:

Corollary D. *Let G denote the group scheme corresponding to the p-torsion of an abelian variety of dimension 3 with p-rank 0 and a-number 1. For $p = 3, 5, 7$, there is a hyperelliptic curve C of genus 4 such that*

$$\mathrm{Jac}(C)[p] = G \oplus (\mathbf{Z}/p \oplus \mu_p).$$

For $p = 3, 5$, there is a hyperelliptic curve C of genus 5 such that

$$\mathrm{Jac}(C)[p] = G \oplus (\mathbf{Z}/p \oplus \mu_p)^2.$$

Our main obstruction to extending these results to higher primes and genus is twofold: first, the formulae obtained are inhumanely complicated, even at small primes; second, the Magma code written is not optimal. The latter problem should be something which can be easily fixed. This may allow for extensions of the above results.

1.1. **Acknowledgements.** We would like to thank David Zureick-Brown for suggesting this project, and the Emory REU for allowing us to conduct this research. We thank David Zureick-Brown, Jackson Morrow, and Rachel Pries for comments on a draft. Thanks to many people, Emory was an intellectually stimulating environment: we are particularly grateful to Noam Kantor, Jackson Morrow, Ken Ono, and David Zureick-Brown. We would also like to thank Rachel Pries and Sammy Luo for helpful discussions regarding the topic of this paper. Lastly, we'd like to thank the other participants in the Emory REU for making our summer fun and enjoyable.

This research was supported by the Templeton World Charity Foundation and NSF Grant DMS-1557690.

2. Background

2.1. **The Hasse invariant.**

2.1.1. *Elliptic curves.* Let E be an elliptic curve defined by $y^2 = f(x)$ over a field k of characteristic p. There are multiple ways to state that E is ordinary, some of which are as follows.

- We have $E[p^k] \simeq \mathbf{Z}/p^k$ for all k.
- The trace of Frobenius on E is nonzero.
- The Newton polygon of E is "as low as possible", i.e., has a line of slope -1 from $(0, 1)$ to $(1, 0)$, and has a line of slope 0 from $(1, 0)$ to $(2, 0)$.
- The formal group associated to E is of height 1, i.e., is isogenous to $\mathbf{G}_m$.
- Let H_p denote the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$. This is known as the *Hasse invariant*. Then $H_p \neq 0$.

We will be interested in generalizations to higher-dimensional abelian varieties of the last characterization.

The Hasse invariant is easy to compute, but its significance is opaque. To explain the definition, we need to set some notation. Let F denote the Frobenius on E; this is a morphism of schemes $E \to E^{(p)}$. The dual of this is the Verschiebung, which is a morphism $V : E^{(p)} \to E$.

The Verschiebung induces a morphism on (co)tangent spaces, and in particular, gives a morphism $V\colon \Omega^1_K \to \Omega^1_{K^p}$, where $K = K(E)$ and K^p is $K(E^{(p)})$. (Note that the Frobenius also gives a morphism $\Omega^1_{K^p} \to \Omega^1_K$.) We can compute this map V explicitly by fixing a nice basis for the differential forms of degree 1 and of the first kind (these are exactly the global sections of Ω^1_E). This is just a one-dimensional k-vector space, so we may choose the basis consisting of the vector $dx/y \coloneqq \omega$.

To determine V, it suffices to determine $V(\omega)$. Explicitly, we find that we can write any element of Ω^1_K in the form $d\phi + \eta^p x^{p-1} dx$, where $\phi, \eta \in K$ and $\eta^p \in K^p$, and that

$$V(d\phi + \eta^p x^{p-1} dx) = \eta \; dx;$$

this is exactly as one would expect the Verschiebung to behave, since it is dual to the Frobenius. Computing $V(\omega)$ will be a moment away if we can write ω in this form. Define c_i by the expansion

$$f(x)^{(p-1)/2} = \sum_{j=0}^{3(p-1)/2} c_j x^j dx.$$

Then (as in [Sil09, §V.4])

$$\omega = y^{-p} \left(y^2\right)^{(p-1)/2} dx = y^{-p} \sum_{j=0}^{3(p-1)/2} c_j x^j dx.$$

One can then compute (we will do this in more generality below) that

$$V(\omega) = c_p^{1/p} dx/y.$$

Similarly, one finds that $F(\omega) = c_p d^p x^p / y^p$, where $d^p\colon K^p \to \Omega^1_{K^p}$ is the universal derivation.

In particular, the nonvanishing of the Hasse invariant is equivalent to V inducing a nonzero map on tangent spaces. This means that the multiplication-by-p map (which is the Verschiebung composed with the Frobenius) will have seperable degree p — and one can show that this is equivalent to $E[p]$ having p connected components.

2.1.2. *Hyperelliptic curves.* The method of generalization to hyperelliptic curves is an exact analogue of the above. We follow [Yui78]. Let $C\colon y^2 = f(x)$ now be a hyperelliptic curve of genus g, so that the degree of f is $2g+1$ or $2g+2$. Then – exactly as above – we can consider the effect of the Verschiebung and the Frobenius on the sheaf of Kahler differentials.

This gives the "modified Cartier" and the "Cartier" operators, respectively. We may pick the basis (as a k-vector space) for the global sections of Ω^1_C given by

$$\omega_i \coloneqq x^{i-1} dx/y,$$

for $1 \le i \le g$. Then, we can rewrite

$$\omega_i = y^{-p} x^{i-1} \sum_{j=0}^{(p-1)/2\cdot(2g+1)} c_j x^j dx,$$

and attempt to compute the effect of applying V and F to each of the basis vectors.

Again, we find that we can write any element of Ω^1_K in the form $d\phi + \eta^p x^{p-1} dx$, where $\phi, \eta \in K$ and $\eta^p \in K^p$, and that V sends this to $\eta \; dx$.

Lemma 2.1. *The action of F and V on $\mathrm{H}^0(C, \Omega^1_C)$ is determined by the following equations:*

$$V(\omega_i) = \sum_{j=0}^{g-1} c^{1/p}_{(j+1)p-i} \frac{x^j}{y} dx, \tag{1}$$

$$F(\omega_i) = 0. \tag{2}$$

Proof. It is clear that $F(\omega_i) = 0$, so we will just compute $V(\omega_i)$. This computation will be immediate if we can write ω_i in the form $d\phi + \eta^p x^{p-1} dx$, which we can do: since

$$\omega_i = y^{-p} \left(\sum_{j=0}^{(p-1)/2\cdot(2g+1)} c_j x^{j+i-1} \right) dx,$$

we get

$$\begin{aligned} \omega_i &= y^{-p} \left(\sum_{i+j \neq 0 \mod p} c_j x^{j+i-1} \right) + y^{-p} \left(\sum_j c_{(j+1)p-i} x^{(j+1)p-1} dx \right) \\ &= d \left(y^{-p} \sum_{i+j \neq 0 \mod p} \frac{c_j}{j+i} x^{j+i} \right) + \sum_j c_{(j+1)p-i} \frac{x^{jp}}{y^p} x^{p-1} dx. \end{aligned}$$

It follows that

$$V(\omega_i) = \sum_{j=0}^{g-1} c_{(j+1)p-i}^{1/p} \frac{x^j}{y} dx,$$

as desired. □

Define a matrix A via $A_{i,j} \coloneqq c_{ip-j}$; then, Lemma 2.1 implies that if $A^{(1/p)}$ denotes the matrix such that $A^{(1/p)}_{i,j} = (A_{i,j})^{1/p}$, the Verschiebung V acts via $A^{(1/p)}$. This matrix is called the *Hasse–Witt matrix*. It is clear that the Hasse–Witt matrix of C is unique up to transformations of the form $A \mapsto S^{(p)} A S^{-1}$, where $S^{(p)}_{i,j} \coloneqq (S_{i,j})^p$.

As an example of how the Hasse–Witt matrix may be used to detect supersingularity, we state the following theorem of Yui.

Theorem 2.2 ([Yui78]). *Let C be a hyperelliptic curve of genus g over k. If the Hasse–Witt matrix of C is 0 in k, then the Jacobian $J(C)$ is superspecial and is isogenous to g copies of a supersingular curve (over some finite extension of k).*

2.2. **de Rham cohomology.** Notice that F and V both take exact forms to zero. (In fact, F takes all forms to 0.) In fact, the Hasse–Witt matrix A is exactly the matrix (in the basis written down above) for the action of the Frobenius on $\mathrm{H}^1(C, \mathscr{O}_C)$. Equivalently, by Serre duality, it is the matrix of the Verschiebung on the zeroth cohomology of the de Rham complex.

There is a larger vector space which contains more information than just $\mathrm{H}^1(C, \mathscr{O}_C)$ and $\mathrm{H}^0(C, \Omega^1_C)$. This is the (first) de Rham cohomology of C. Recall that the Hodge–de Rham spectral sequence runs

$$E_1^{p,q} = \mathrm{H}^p(X, \Omega^p_{X/K}) \Rightarrow \mathrm{H}^{p+q}_{\mathrm{dR}}(X).$$

The resulting filtration on $\mathrm{H}^*_{\mathrm{dR}}(X)$ is called the *Hodge filtration*. An important, well-known theorem, is the following:

Theorem 2.3. *The Hodge–de Rham spectral sequence collapses at the E_1-page if X is smooth and proper.*

The associated graded of the Hodge filtration is exactly given by

$$\mathrm{gr}^p \mathrm{H}^i_{\mathrm{dR}}(X) = \mathrm{H}^{i-p}(X, \Omega^p_{X/K}).$$

Let $\mathrm{H}^{p,q} = \dim_K \mathrm{H}^q(X, \Omega^p_{X/K})$; then Serre duality gives an equality $\mathrm{H}^{p,q} = \mathrm{H}^{n-p,n-q}$, where n is the dimension of X. One also has "conjugation symmetry", which says that $\mathrm{H}^{p,q} = \mathrm{H}^{q,p}$.

We can, in particular, consider the Hodge filtration for $\mathrm{H}^1_{\mathrm{dR}}(X)$. Given the description above, we obtain a short exact sequence

$$0 \to \mathrm{H}^0(X, \Omega^1_{X/R}) \simeq \mathrm{gr}^1 \mathrm{H}^1_{\mathrm{dR}}(X) \to \mathrm{H}^1_{\mathrm{dR}}(X) \to \mathrm{gr}^0 \mathrm{H}^1_{\mathrm{dR}}(X) \simeq \mathrm{H}^1(X, \mathscr{O}_X) \to 0.$$

The two associated gradeds are of the same dimension.

As above, suppose that $X = C$ is a smooth geometrically connected projective hyperelliptic curve over k of genus g. It follows from GAGA that $\mathrm{H}^1_{\mathrm{dR}}(C)$ is a $2g$-dimensional k-vector space. Since C lives over k, we still have an action of F and V on $\mathrm{H}^1_{\mathrm{dR}}(C)$. The rest of this paper is devoted to finding explicit formulae for this action.

3. The Dieudonné module of Jacobians

In this section, we will prove Theorem A and Theorem B.

3.1. **A basis for the first de Rham cohomology group.** Let C be a hyperelliptic curve defined by an equation $y^2 = f(x)$ over a perfect field k of odd characteristic p, where $f(x)$ is a separable polynomial of degree d. By standard arguments (see [Poo06, §2.8]) if d is odd we have that $d = 2g+1$ where g is the genus, and if d is even we have that $d = 2g+2$. If we let $\mathbf{A}^1_x$ and $\mathbf{A}^1_u$ be the standard affine charts on $\mathbf{P}^1$, where $u = 1/x$, we have that C is defined over $\mathbf{A}^1_x$ by the equation $y^2 = f(x)$, and over $\mathbf{A}^1_u$ by the equation $v^2 = u^{2g+2} f(1/u)$, glued together by setting $v = y/x^{g+1}$. Let $\pi \colon C \to \mathbf{P}^1$ be the projection. Let $P_0 = [0:1]$ and $P_\infty = [1:0]$.

On C,

$$(x) = \pi^* P_0 - \pi^* P_\infty.$$

If d is odd, this means there will be a single point of C above P_∞, so x will have a pole of order 2 there, and if d is even, (x) will have a pole of order 1 at each of the two $\bar{k}$ points above P_∞. Whether d is even or odd, we know that

$$(dx/y) = (g-1)\pi^* P_\infty,$$

as in [Poo06, §2.8]. If d is odd, y will have a pole of order $d = 2g+1$ above P_∞, and if d is even, (y) above infinity will look like $(g+1)\pi^* P_\infty$.

Recall that a canonical basis for $\mathrm{H}^0(C, \Omega^1_C)$ is given by the 1-forms $\tau_{i-1} = x^{i-1} dx/y$ for i ranging between 1 and g. To compute a basis for $\mathrm{H}^1(C, \mathscr{O}_C)$, we use the two term Cech cover $\mathscr{C}$ given by $U = \pi^{-1}(\mathbf{A}^1_u)$ and $V = \pi^{-1}(\mathbf{A}^1_x)$. Moreover,

$$U \cap V = \operatorname{Spec} k[x, y, x^{-1}]/(y^2 - f(x)),$$

so $\Gamma(U \cap V, \mathscr{O}_{U\cap V})$ has a basis given by $\{x^i\}_{i \in \mathbf{Z}} \cup \{yx^j\}_{j \in \mathbf{Z}}$.

Similarly,

$$\Gamma(V, \mathscr{O}_V) = k[x, y]/(y^2 - f)$$

has a basis given by x^i for all non-negative i and yx^j for all nonnegative j. $\Gamma(U, \mathscr{O}_U) = k[x^{-1}, yx^{-(g+1)}]/(y^2 - f)$ has a basis given by x^i for all non-positive i and yx^j for all $j \leq -(g+1)$. Thus the basis vectors of

$$\mathrm{H}^1(C, \mathscr{O}_C) = \Gamma(U \cap V, \mathscr{O}_{U \cap V}) / \Gamma(U, \mathscr{O}_U) \oplus \Gamma(V, \mathscr{O}_V)$$

consist of $\{y/x^j\}_{j=1,\ldots,g}$.

We can now extend the bases of $\mathrm{H}^0(C, \Omega^1_C)$ and $\mathrm{H}^1(C, \mathscr{O})$ to a basis of $\mathrm{H}^1_{\mathrm{dR}}(C, \mathscr{C})$. We begin by noting that the basis of $\mathrm{H}^0(C, \Omega^1_C)$ can be easily extended by defining

$$\widetilde{\tau}_i = \left(x^i \frac{dx}{y}, x^i \frac{dx}{y}, 0 \right),$$

as i ranges from 0 to $g-1$.

To extend the basis $\mathrm{H}^1(C, \mathscr{O}_C)$ we will write out the polynomial for $f(x)$ as

$$f(x) = \sum_{k=0}^{d} a_k x^k.$$

We can then compute:

$$\begin{aligned} d(y/x^j) &= \frac{dy}{x^j} - j\frac{ydx}{x^{j+1}} \\ &= \frac{1}{x^j}\left(\frac{f'}{2y} - j\frac{y}{x}\right) dx \\ &= \frac{1}{x^j}\left(f'(x) - 2jf(x)/x\right)\frac{dx}{2y} \\ &= \sum_{k=0}^{d}(k-2j)a_k x^{k-j-1}\frac{dx}{2y}. \end{aligned}$$

Motivated by this, define differential forms (for j ranging between 1 and g)

$$\begin{aligned} \omega_1^{(j)} &= \sum_{k=0}^{j}(k-2j)a_k x^{k-j-1}\frac{dx}{2y}, \\ \omega_2^{(j)} &= -\left(\sum_{j+1}^{d}(k-2j)a_k x^{k-j-1}\frac{dx}{2y}\right). \end{aligned}$$

As dx/y is regular and $\omega_1^{(j)}$ is the product of a polynomial in $1/x$ and $\frac{dx}{y}$, $\omega_1^{(j)}$ has a pole only at 0. A similar argument proves that ω_2 has a pole only at ∞. This discussion implies:

Theorem A. The elements $(\omega_1^{(j)}, \omega_2^{(j)}, yx^{-j}) = \widetilde{\eta}_i$ for $1 \le j \le g$, along with the elements $\widetilde{\tau}_i$ for $0 \le i \le g-1$, form a basis for $\mathrm{H}^1_{\mathrm{dR}}(C)$.

Let $j \le 0$. Then y/x^j is a polynomial in x and y, and the above computation shows that $d(y/x^j)$ is regular everywhere on V, and has poles only above P_∞. Define

$$\begin{aligned} \omega_1^{(j)} &= 0, \\ \omega_2^{(j)} &= -d(y/x^j) = -\left(\sum_{k=0}^{d}(k-2j)a_k x^{k-j-1}\frac{dx}{2y}\right). \end{aligned}$$

For $j \ge g+1$, consider the differential form

$$\widetilde{\omega}^{(j)} = d(y/x^j) = \sum_{k=0}^{d}(k-2j)a_k x^{k-j-1}\frac{dx}{2y}.$$

This is defined differently from the other differential forms $\omega_1^{(j)}$, because the sum ranges from 1 to d. This means that if $j < d$, there will be some positive terms of x in the sum. Since the largest power of x is x^{d-j-1} (which has order $-2d+2+2j$ over P_∞), and dx/y has a zero of order $2g-2$ over P_∞ [2] we have

$$\left(x^{d-j-1}\frac{dx}{y}\right)_{P_\infty} = 2g-2-2d+2+2j = 2(g-d)+2j = 2j-2(d-g).$$

[2] In the case that d is even and there are two points over P_∞, both x and dx/y will in fact have two poles resp. zeroes of the same degree over each of the points over P_∞, so to prove a function is regular it suffices to prove that the total valuation over P_∞ is positive, which we denote by $(\cdot)_{P_\infty}$.

If d is odd, $d-g=g+1$, and since $j \geq g+1$, this is regular at P_∞; hence $\widetilde{\omega}^{(j)}$ is a well-defined element of $\Gamma(U, \Omega^1_C)$. If d is even, $d-g=g+2$, so the only case where this might have poles over P_∞ is if $j=g+1$. But note that the coefficient of x^{d-j-1} is $d-2j$, so if $j=g+1$, $d-2j=0$ and this term vanishes. Thus in either case we have a well-defined element of $\Omega^1_C(U)$.

Using the basis determined here, we can compute the action of Verschiebung and Frobenius on $\mathrm{H}^1_{\mathrm{dR}}(C)$.

3.2. **The Verschiebung action.** To ease notation, let us redefine

$$\widetilde{\tau}_i = \left(x^i \frac{dx}{y}, x^i \frac{dx}{y}, 0 \right),$$

as i ranges from 1 through g.

We kick off by noting that the Verschiebung is trivial on $\mathrm{H}^1(C, \mathscr{O}_C)$, simply because of Serre duality (the Frobenius is trivial on $\mathrm{H}^0(C, \Omega^1_C)$). Thus we only have to compute the Verschiebung action on $\omega_1^{(j)}$ and $\omega_2^{(j)}$, for $j = 1, \ldots, g$. Note that the Verschiebung takes exact forms to zero, and hence $V(\omega_1^{(j)}) = -V(\omega_2^{(j)})$; it therefore suffices to compute $V(\omega_1^{(j)})$. This can be written down explicitly:

$$\begin{aligned} V(\omega_1^{(j)}) &= V\left(\sum_{k=0}^{j} (k-2j) a_k x^{k-j-1} \frac{dx}{2y} \right) \\ &= \sum_{k=0}^{j} (k-2j) a_k^{1/p} V\left(x^{k-j-1} \frac{dx}{2y} \right). \end{aligned}$$

At this point, the computation is exactly that done in Lemma 2.1: we can write

$$\begin{aligned} V(\omega_1^{(j)}) &= \sum_{k=1}^{j} (k-2j) a_k^{1/p} \sum_{i=1}^{g} c_{ip-k+j}^{1/p} \frac{x^i}{2y} dx \\ &= \sum_{i=1}^{g} \sum_{k=1}^{j} \frac{(k-2j)}{2} a_k^{1/p} c_{ip-k+j}^{1/p} \frac{x^i}{y} dx. \end{aligned}$$

In the basis $(\widetilde{\eta}_1, \cdots, \widetilde{\eta}_g, \widetilde{\tau}_1, \cdots, \widetilde{\tau}_g)$, the matrix of Verschiebung is therefore determined by the following facts:

- The coefficient of $\widetilde{\eta}_i$ in $V(\widetilde{\eta}_j)$ is zero.
- The coefficient of $\widetilde{\tau}_i$ in $V(\eta_j)$ is
$$\sum_{k=0}^{j} (k-2j) a_k^{1/p} c_{ip-k+j}^{1/p}.$$
- The coefficient of $\widetilde{\eta}_i$ in $V(\widetilde{\tau}_j)$ is zero.
- The coefficient of $\widetilde{\tau}_i$ in $V(\widetilde{\tau}_j)$ is given by $c_{ip-j}^{1/p}$.

We can now graduate to a harder computation.

3.3. **The Frobenius action.** Because $d(x^p) = px^{p-1}dx = 0$, we have

$$F(\widetilde{\tau}_i) = 0.$$

Similarly,

$$F(\omega_1^{(j)}, \omega_2^{(j)}, y/x^j) = (0, 0, y^p x^{-pj}).$$

Write

$$f(x)^{\frac{p-1}{2}} = \sum_{k=0}^{N} c_k x^k,$$

where $N = d(p-1)/2$, so that

$$y^p x^{-pj} = y(y^2)^{(p-1)/2} x^{-pj} = y \sum_{k=0}^{N} c_k x^{k-pj}.$$

If we let $i = pj - k$, then

$$F(yx^{-j}) = y^p x^{-pj} = \sum_{i=pj-N}^{pj} c_{pj-i} y/x^i.$$

For all $i \in \{1, \dots, g\}$, we subtract $c_{pj-i}\widetilde{\eta}_i$ from the sum to we get an element of the form

$$\left(\sum_{i=1}^{g} -c_{pj-i}\omega_1^{(i)}, \sum_{i=1}^{g} -c_{pj-i}\omega_2^{(i)}, \sum_{i \notin \{1,\dots,g\}} c_{pj-i} y/x^i \right).$$

Note that *a priori*, we should be looking at $i \geq \max\{pj - N, 1\}$, but if $pj - N > i$, then $pj - i > N$; so if we set $c_k = 0$ for $k > N$, we can just subtract $c_{pj-i}\widetilde{\eta}_i$ for $i = 1, \dots, g$.

All of the remaining i in the sum are either less than 1 or greater than g, so we know that $(0, \omega_2^{(i)}, y/x_i)$ is a coboundary for $i \leq 0$, and that $(\widetilde{\omega}^{(i)}, 0, y/x_i)$ is a coboundary for $i \geq g+1$. Working in $\mathrm{H}^1_{\mathrm{dR}}(C)$ — i.e., modulo coboundaries — we have:

$$F(\widetilde{\eta}_j) - \sum_{i=1}^{g} c_{pi-i}\widetilde{\eta}_i = \left(\sum_{i=1}^{g} -c_{pj-i}\omega_1^{(i)} + \sum_{i=g+1}^{jp} -c_{pj-i}\widetilde{\omega}^{(i)}, \sum_{i \leq 0} c_{pj-i}\omega_2^{(i)}, 0 \right).$$

Since this is an element of $\mathrm{H}^1_{\mathrm{dR}}(C)$, the difference of the differential forms in the first and second slot must be equal to differential of the third slot; in our case, this implies that the two forms patch up to a globally defined holomorphic differential form. (Note that this implies that all of the negative powers of x and the powers greater than g cancel). We may therefore write:

$$\sum_{i=1}^{g} -c_{pj-i}\omega_1^{(i)} + \sum_{i=g+1}^{jp} -c_{pj-i}\widetilde{\omega}^{(i)} = d_1 \frac{dx}{2y} + d_2 \frac{xdx}{2y} + \cdots + d_g \frac{x^{g-1}dx}{2y}.$$

As both sides of the above equation are holomorphic differential forms, this is an equality of two functions (and not just an equality in cohomology). Since all of the $\omega_1^{(i)}$ are defined such that they have no positive powers of x, the only positive powers of x can come from the ${\omega'}^{(i)}$. We write

$$\begin{aligned} \sum_{i=g+1}^{jp} c_{pj-i}\widetilde{\omega}^{(i)} &= \sum_{i=g+1}^{jp} c_{pj-i} \left(\sum_{k=0}^{d} (k-2i) a_k x^{k-i-1} \right) \frac{dx}{2y} \\ &= \sum_{i=g+1}^{jp} \sum_{k'=-i}^{d-i} c_{pj-i}(k'-i) a_{k'+i} x^{k'-1} \frac{dx}{2y}, \end{aligned}$$

where we set $k' = k - i$. For a fixed $k' \in \{0, \dots, g-1\}$, we therefore have $i \geq \max\{g+1, -k\}$.[3] If $i \geq (j-1)p$, then $pj - i < p$; so $c_{pj-i} = 0$.

It follows that the coefficient of $x^{k'-1}\, dx/2y$ is

$$-\sum_{i=g+1}^{d-k'} c_{pj-i} a_{k'+i}(k'-i).$$

[3] Since $a_{i+k'} = 0$ for $i > d - k'$, the condition that $i \leq d - k'$ is irrelevant.

Thus, in the basis $(\widetilde{\eta}_1, \ldots, \widetilde{\eta}_g, \widetilde{\tau}_1, \ldots, \widetilde{\tau}_g)$, the matrix of Frobenius is completely determined by the following facts:

- The $\widetilde{\eta}_i$ coefficient of $F(\widetilde{\eta}_j)$ is c_{pj-i}.
- The $\widetilde{\tau}_i$ coefficient of $F(\widetilde{\eta}_j)$ is
$$\sum_{k=g+1}^{d-i} (k-i)c_{pj-k}a_{k+i}.$$
- The $\widetilde{\eta}_i$ coefficient of $F(\widetilde{\tau}_j)$ is zero.
- The $\widetilde{\tau}_i$ coefficient of $F(\widetilde{\tau}_j)$ is zero.

Combining the result of the last section, we obtain Theorem B.

4. Applications

Using the computations in the previous section, we can compute the matrix for the Frobenius and Verschiebung on the Jacobian of any hyperelliptic curve, as well as the Ekedahl–Oort type. The computations done below were performed with the use of `Magma`; the code utilized is available at https://github.com/sanathdevalapurkar/dieudonne-modules.

4.1. **A note on the curves $y^2 = x^d + 1$.** From our code, we discovered an interesting pattern regarding the $p-$rank of curves of the form $y^2 = x^d + 1$ modulo various primes p in the case d is also a prime. They will always be ordinary in the case that $p = 1 \pmod d$, but if $p \neq 1 \pmod d$ they will often have very low $p-$rank. The strongest result occurs when both d and $g = \frac{d-1}{2}$ are prime.

Theorem C. Let d be an odd prime such that $g = \frac{d-1}{2}$ is also prime. Let p be a prime not equal to d. Then the Jacobian of the hyperelliptic curve $y^2 = x^d + 1$ is ordinary if $p \equiv 1 \pmod d$, and has p-rank 0 if $p \not\equiv 1 \pmod d$.

Proof. Recall that the p-rank of a hyperelliptic curve is equal to the limiting rank of the Hasse–Witt matrix H, defined by $H_{i,j} = c_{pi-j}$ where
$$\sum_k c_k x^k = (x^d + 1)^{(p-1)/2}.$$
Thus we have that
$$c_{rd} = \binom{(p-1)/2}{r},$$
and c_k is zero for k not a multiple of d.

Suppose $p \equiv 1 \pmod d$, and set $p = md + 1$. We have that
$$H_{i,i} = \binom{(p-1)/2}{mi}.$$
Since $i \le g = (d-1)/2$ it is easy to check that $(p-1)/2 > mg$, and therefore the matrix has nonzero entries on the diagonal. Since $i, j \in \{1, \ldots, g\}$ and $pi - j \equiv i - j \pmod d$, we can only have $d \mid pi - j$ if $i = j$. Thus there can be no other nonzero entries, so H is an invertible diagonal matrix and C is ordinary.

Suppose $p \not\equiv 1 \pmod d$. Assume that $p \equiv -1 \pmod d$. Then $pi - j \equiv -(i+j) \pmod d$, and since i and j range from 1 to g, the sum $i + j$ ranges from 2 to $2g$ and so can never be 0 mod d. Thus c_{pi-j} is zero for all entries and the Hasse–Witt matrix is identically 0, so in particular C has p-rank 0.

The remaining case is when p is neither 1 nor -1 mod d. Then we claim H will be nilpotent, which is equivalent to having characteristic polynomial $P_H(T) = T^g$. We write

$$P_H(T) = \det(TI - H) = \sum_{\sigma \in S_n} \prod_{i=1}^{g} (\delta_{i,\sigma(i)} T - H_{i,\sigma(i)}).$$

Since we know that $pi - i = (p-1)i$ cannot be 0 mod d, we know that $H_{i,i} = 0$, and so the coefficient of T^k will be a sum of products $\prod_{i \notin \mathrm{Fix}(\sigma)} H_{i,\sigma(i)}$, where σ fixes k points and the product now ranges only over the elements not fixed by σ. To prove this equals T^n, it suffices to show that for any nontrivial cycle $(\alpha_1, \ldots, \alpha_k)$, we have

$$\prod_{i=1}^{k} H_{\alpha_i, \alpha_{i+1}} = 0.$$

Consider such a cycle, and suppose the above product is not 0. Then we have that $p\alpha_i - \alpha_{i+1} \equiv 0 \pmod{d}$, and therefore $p\alpha_i \equiv \alpha_{i+1} \pmod{d}$ for all i, and $p\alpha_k \equiv \alpha_i \pmod{d}$. Therefore $p^k \equiv 1 \pmod{d}$, so p must have order k in $(\mathbf{Z}/d)^\times$. Since d is prime, this is the cyclic group $\mathbf{Z}/2g$, and since g is prime this means $k \in \{1, 2, g, 2g\}$. The cycle clearly cannot have length $2g$, and since $p \not\equiv 1$ or -1 it cannot have order 1 or 2, so the only important case is $k = g$. If the product $\prod_{i=1}^{n} H_{i,\sigma(i)}$ over a cycle of length g was nonzero, it would imply in particular that each row of H has a nonzero element.

But if $p \not\equiv 1 \pmod{d}$, this is impossible, because there will be some $i \in \{1, \ldots, g\}$ such that pi mod d lies between $g+1$ and $2g$. Then for such an i, $pi - j$ will never be 0 mod d for $j \in \{1, \ldots, g\}$, so the ith row of H will be zero. Thus H has characteristic polynomial T^g, so is nilpotent, and so C has p-rank 0. □

4.2. **Distribution of final types for low primes.** At low primes, we can count the number of final types coming from hyperelliptic curves. The data presented below is written in the form

`<final type, number of copies>.`

```
Degree: 3
Prime: 3
The number of final types coming from hyperelliptic curves is 2 (out of 2
possibilities).

{
    <[ 0 ], 12>,
    <[ 1 ], 24>
}
Time taken: 0.010
------------------------------------------------------------
Degree: 5
Prime: 3
The number of final types coming from hyperelliptic curves is 3 (out of 4
possibilities).

{
    <[ 0, 1 ], 36>,
    <[ 1, 2 ], 240>,
    <[ 1, 1 ], 48>
}
Time taken: 0.170
------------------------------------------------------------
```

```
Degree: 7
Prime: 3
The number of final types coming from hyperelliptic curves is 4 (out of 8
possibilities).

{
    <[ 1, 2, 2 ], 684>,
    <[ 1, 2, 3 ], 1884>,
    <[ 1, 1, 2 ], 240>,
    <[ 0, 1, 2 ], 108>
}
Time taken: 5.400
-------------------------------------------------------------
Degree: 9
Prime: 3
The number of final types coming from hyperelliptic curves is 11 (out of 16
possibilities).

{
    <[ 1, 1, 2, 3 ], 528>,
    <[ 0, 1, 2, 2 ], 48>,
    <[ 1, 1, 2, 2 ], 240>,
    <[ 1, 2, 2, 3 ], 1920>,
    <[ 1, 2, 3, 3 ], 5232>,
    <[ 0, 1, 2, 3 ], 204>,
    <[ 0, 1, 1, 2 ], 48>,
    <[ 0, 0, 1, 2 ], 12>,
    <[ 1, 2, 2, 2 ], 576>,
    <[ 1, 2, 3, 4 ], 17388>,
    <[ 1, 1, 1, 2 ], 48>
}
Time taken: 363.380
-------------------------------------------------------------
Degree: 3
Prime: 5
The number of final types coming from hyperelliptic curves is 2 (out of 2
possibilities).

{
    <[ 1 ], 320>,
    <[ 0 ], 80>
}
Time taken: 0.170
-------------------------------------------------------------
Degree: 5
Prime: 5
The number of final types coming from hyperelliptic curves is 4 (out of 4
possibilities).

{
    <[ 0, 1 ], 240>,
    <[ 1, 1 ], 1760>,
    <[ 1, 2 ], 7920>,
    <[ 0, 0 ], 80>
```

```
}
Time taken: 50.920
```

Our algorithm is not optimal; one should be able to write a faster algorithm to gather more data for higher primes and larger genus.

4.3. **A question of Glass-Pries.** Let G be the group scheme corresponding to the p-torsion of an abelian variety of dimension 3 with p-rank 0 and a-number 1. One can show that

$$D(G) \simeq k[F,V]/(F^4, V^4, F^3 - V^3),$$

where $D(G)$ is the Dieudonné module of G.

In [Cor05, Question 5.9], Glass and Pries ask the following question.

Question 2. Are there smooth hyperelliptic curves C and D of genus 4 and 5, respectively, such that

$$\mathrm{Jac}(C) \simeq G \oplus (\mathbf{Z}/p \oplus \mu_p), \text{ and } \mathrm{Jac}(C') \simeq Q \oplus (\mathbf{Z}/p \oplus \mu_p)^2?$$

We can answer this question in the affirmative for small primes using our Magma code. A simple linear algebra exercise allows one to compute the matrices for the Frobenius and Verschiebung. Using our code, this allows us to determine the canonical type:

	Canonical type
$G \oplus (\mathbf{Z}/p \oplus \mu_p)$	$[1,1,2,3]$
$G \oplus (\mathbf{Z}/p \oplus \mu_p)^2$	$[1,2,2,3,4]$

By running through all possible (smooth) hyperelliptic curves, and comparing the associated canonical types, we can find the desired curves. For genus 4, we find that the following hyperelliptic curves answer Question 2, thus proving Corollary D:

- At $p=3$: the curve
$$y^2 = 2x^9 + x^8 + x.$$
- At $p=5$: the curve
$$y^2 = x^9 + x^8 + x.$$
- At $p=7$: the curve
$$y^2 = 5x^9 + 3x^7 + x^6 + x.$$

For genus 5, we find that the following hyperelliptic curves answer Question 2:

- At $p=3$: the curve
$$y^2 = 2x^{11} + x^9 + x^7 + x.$$
- At $p=5$: the curve
$$y^2 = 3x^{11} + 2x^{10} + 4x^9 + 2x^8 + x^7 + x.$$

References

[Cor05] Cornelissen, G. and Oort, F. and Chinburg, T. and Gasbarri, C. and Glass, D. and Lehr, C. and Matignon, M. and Pries, R. and Wewers, S. Problems from the Workshop on Automorphisms of Curves; chapter titled "Questions on p-torsion of hyperelliptic curves". *Rend. Sem. Mat. Univ. Padova*, 113:129–177, 2005. (Cited on pages 1, 4, and 14.)

[EP13] A. Elkin and R. Pries. Ekedahl–Oort strata of hyperelliptic curves in characteristic 2. *Algebra and Number Theory*, 7(3):507–532, 2013. (Cited on pages 2 and 3.)

[Oda69] T. Oda. The first de Rham cohomology group and Dieudonné modules. *Ann. Sci. Ecole Norm. Sup.*, 4(2):63–135, 1969. (Cited on pages 1 and 2.)

[Poo06] B. Poonen. Lectures on rational points on curves. http://math.mit.edu/~poonen/papers/curves.pdf, March 2006. (Cited on page 7.)

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009. (Cited on page 5.)

[Yui78] N. Yui. On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$. *J. Algebra*, 52(2):378–410, 1978. (Cited on pages 5 and 6.)

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02142
Email address: sanathd@mit.edu

Department of Mathematics, University of Chicago, 5801 S Ellis Ave, Chicago, IL 60637
Email address: jhalliday@uchicago.edu