Asian J. Math.
Vol. 19, No. 5, pp. 845–870, November 2015

003

THE EKEDAHL-OORT TYPE OF JACOBIANS OF HERMITIAN CURVES*

RACHEL PRIES† AND COLIN WEIR‡

Abstract. The Ekedahl-Oort type is a combinatorial invariant of a principally polarized abelian variety A defined over an algebraically closed field of characteristic $p > 0$. It characterizes the p-torsion group scheme of A up to isomorphism. Equivalently, it characterizes (the mod p reduction of) the Dieudonné module of A or the de Rham cohomology of A as modules under the Frobenius and Vershiebung operators.

There are very few results about which Ekedahl-Oort types occur for Jacobians of curves. In this paper, we consider the class of Hermitian curves, indexed by a prime power $q = p^n$, which are supersingular curves well-known for their exceptional arithmetic properties. We determine the Ekedahl-Oort types of the Jacobians of all Hermitian curves. An interesting feature is that their indecomposable factors are determined by the orbits of the multiplication-by-two map on $\mathbb{Z}/(2^n+1)$, and thus do not depend on p. This yields applications about the decomposition of the Jacobians of Hermitian curves up to isomorphism.

Key words. Hermitian curve, maximal curve, Jacobian, supersingular, Dieudonné module, p-torsion, de Rham cohomology, Ekedahl-Oort type, a-number, Selmer group.

AMS subject classifications. 11G20, 14G50, 14H40.

1. Introduction.

A crucial fact about a principally polarized abelian variety A defined over an algebraically closed field k of characteristic $p > 0$ is that the multiplication-by-p morphism of A is inseparable. If A has dimension g, then $[p]$ factors as $V \circ F$ where the Frobenius morphism F is purely inseparable of degree p^g and where V is the Verschiebung morphism. The isomorphism class of the p-torsion group scheme $A[p]$ is determined by the interaction between F and V. It can be characterized by its Ekedahl-Oort type or by the structure of its Dieudonné module. There are many deep results about the stratification of the moduli space $\mathcal{A}_g$ of principally polarized abelian varieties by Ekedahl-Oort type, see especially [Oor01] and [EvdG09].

In contrast, there are almost no results about which Ekedahl-Oort types occur for Jacobians of curves. There are existence results for Ekedahl-Oort types of low codimension, for which the Jacobians are close to being ordinary [Pri09]. There is a complete classification for hyperelliptic curves when $p = 2$ [EP13].

In this paper, we determine the Ekedahl-Oort type of the Hermitian curve X_q for every prime power q, see Theorem 5.13. More precisely, we determine the structure and multiplicity of each indecomposable factor of the Dieudonné module for the p-torsion group scheme of the Jacobian of X_q. For the proof, we compute the module structure of $H^1_{\mathrm{dR}}(X_q)$ under F and V. The Hermitian curves are remarkable for their properties over finite fields, but the Ekedahl-Oort type and the Dieudonné module are geometric invariants. Thus we work over $k = \overline{\mathbb{F}}_p$ throughout the paper.

This introduction contains: (1.1) a review of the arithmetic properties of Hermitian curves; (1.2) a result of Ekedahl that is the starting point for this work; (1.3) a description of the main result, Theorem 5.13; (1.4) an overview of some applications of this result to questions about the isomorphism class of Jacobians of Hermitian curves,

*Received April 23, 2013; accepted for publication April 17, 2014.
†Colorado State University, Fort Collins, CO, United States 80521 (pries@math.colostate.edu).
‡Simon Fraser University, Burnaby, BC, Canada V5A1S6 (colin_weir@sfu.ca).

about Selmer groups, and about the supersingular locus of $\mathcal{A}_g$; (1.5) a comparison with earlier work; and (1.6) an outline of the rest of the paper.

1.1. Hermitian curves. The Hermitian curves have received much scrutiny for their remarkable arithmetic properties and applications to combinatorics and coding theory. For a prime power $q = p^n$, the *Hermitian curve* X_q is the curve in $\mathbb{P}^2$ defined over $\mathbb{F}_p$ by the homogenization of the equation

$$X_q : y^q + y = x^{q+1}.$$

The curve X_q is smooth and irreducible with genus $g = q(q-1)/2$ and it has exactly one point P_∞ at infinity. The number of points on the Hermitian curve over $\mathbb{F}_{q^2}$ is $\#X_q\left(\mathbb{F}_{q^2}\right) = q^3+1$ and the curve X_q is maximal over $\mathbb{F}_{q^2}$ [Sti09, VI 4.4]. In fact, X_q is the unique curve of genus g which is maximal over $\mathbb{F}_{q^2}$ [RS94]. This implies that X_q is the Deligne-Lusztig variety of dimension 1 associated with the group $G = \mathrm{PGU}(3, q)$ [Han92, Proposition 3.2]. The automorphism group of X_q is G, which has order $q^3(q^2-1)(q^3+1)$, see [GSX00, Equation 2.1]; the Hermitian curves are the only exceptions to the bound of $16g^4$ for the order of the automorphism group of a curve in positive characteristic [Sti73]. They can be characterized as certain ray class fields [Lau99].

The zeta function of X_q is

$$Z(X_q/\mathbb{F}_q, t) = \frac{(1+qt^2)^g}{(1-t)(1-qt)},$$

[Han92, Proposition 3.3] and the only slope of the Newton polygon of the L-polynomial $L(t) = (1+qt^2)^g$ is $1/2$. This means that X_q is *supersingular* for every prime power q. The supersingular condition is equivalent to the condition that the Jacobian $\mathrm{Jac}(X_q)$ is isogenous to a product of supersingular elliptic curves [Oor74, Theorem 4.2]. It also implies that $\mathrm{Jac}(X_q)$ has no non-trivial p-torsion points over $\overline{\mathbb{F}}_p$.

1.2. A result of Ekedahl. It is well-known that the Jacobian of the Hermitian curve $X_p : y^p + y = x^{p+1}$ is *superspecial*, see Section 2.1.4 for definitions. Briefly, the superspecial condition is equivalent to the condition that the Jacobian $\mathrm{Jac}(X_p)$ is isomorphic to a product of supersingular elliptic curves [Oor75, Theorem 2], see also [Nyg81, Theorem 4.1]. Equivalently, (the mod p reduction of) the Dieudonné module of the p-torsion group scheme of $\mathrm{Jac}(X_p)$ is isomorphic to the sum of g copies of the Dieudonné module of a supersingular elliptic curve:

$$\mathbb{D}(\mathrm{Jac}(X_p)) \simeq (\mathbb{E}/\mathbb{E}(F+V))^g. \tag{1}$$

(Here $\mathbb{E} = k[F, V]$ is the non-commutative ring generated by semi-linear operators F and V with the relations $FV = VF = 0$ and $F\lambda = \lambda^p F$ and $\lambda V = V\lambda^p$ for all $\lambda \in k$ and $\mathbb{E}(A_1, \ldots)$ denotes the left ideal of $\mathbb{E}$ generated by $A_1, \ldots$). The easiest way to prove that $\mathrm{Jac}(X_p)$ is superspecial is to show that the Cartier operator is the zero operator on $H^0(X_p, \Omega^1)$, which implies that the kernel of Frobenius F is the kernel of Verschiebung V on the Dieudonné module.

There is an upper bound $g \le p(p-1)/2$ for the genus of a superspecial curve in characteristic p, [Eke87, Theorem 1.1] and this upper bound is realized by X_p. For $n \ge 2$, it is thus impossible for X_q to be superspecial.

1.3. Main result. In this paper, we determine the $\mathbb{E}$-module structure of the Dieudonné module $\mathbb{D}(X_q) := \mathbb{D}(\mathrm{Jac}(X_q)[p])$ for all prime powers $q = p^n$. This is the same as determining the isomorphism class of the p-torsion group scheme of $\mathrm{Jac}(X_q)$. In the main result, see Theorem 5.13, we prove that the distinct indecomposable factors of $\mathbb{D}(X_q)$ are in bijection with orbits of $\mathbb{Z}/(2^n+1) - \{0\}$ under $\langle \times 2 \rangle$ where $\langle \times 2 \rangle$ denotes multiplication-by-two. The structure of each factor is determined by the combinatorics of the orbit, as explained in Section 5.2. In particular, the a-number of each factor is odd. We also determine the multiplicities of the factors. While these multiplicities depend on p, the structure of each indecomposable factor depends only on n. Theorem 5.13 determines the Ekedahl-Oort type ν of $\mathrm{Jac}(X_{p^n})$, although an explicit formula for ν is not easy to write down for general n. In particular, ν has 2^{n-1} *break points* where the behavior of the Ekedahl-Oort sequence switches between the states of being constant and increasing, see Section 2.1.5 and Corollary 5.14.

Examples of $\mathbb{D}(X_{p^n})$ for small n appear in Section 2.2 and Example 5.18. When $n = 2$, the $\langle \times 2 \rangle$ map on $\mathbb{Z}/5 - \{0\}$ has one orbit $\{1, 2, 4, 3\}$. Theorem 5.13 implies that the Dieudonné module of $\mathrm{Jac}(X_{p^2})$ decomposes into $g/2$ copies of the Dieudonné module of a supersingular (but not superspecial) abelian surface:

$$\mathbb{D}(X_{p^2}) = (\mathbb{E}/\mathbb{E}(F^2 + V^2))^{g/2}. \tag{2}$$

For one of the applications, we determine that the $\mathbb{E}$-module $\mathbb{E}/\mathbb{E}(F+V)$ appears as a factor of $\mathbb{D}(X_q)$ if and only if n is odd, in which case it appears with multiplicity $(p(p-1)/2)^n$, see Corollary 5.16.

1.4. Applications. Theorem 5.13 gives partial information about the decomposition of $\mathrm{Jac}(X_q)$, up to isomorphism, into indecomposable abelian varieties, see Section 6.1. For example, when n is a power of 2, we prove that the dimension of each factor in such a decomposition is a multiple of n. For another application, let the *elliptic rank* of an abelian variety A be the largest non-negative integer r such that there exist elliptic curves $E_1, \ldots, E_r$ and an abelian variety B of dimension $g - r$ and an isomorphism $A \simeq B \times (\times_{i=1}^{r} E_i)$ of abelian varieties without polarization.

Application 1.1. *If n is even, then the elliptic rank of* $\mathrm{Jac}(X_{p^n})$ *is* 0. *If n is odd, then the elliptic rank of* $\mathrm{Jac}(X_{p^n})$ *is at most* $(p(p-1)/2)^n$.

The second application is about the Selmer groups for the multiplication-by-p isogeny of a constant elliptic curve E over the function field of a Hermitian curve, see Section 6.2. The third application is about Ekedahl-Oort strata with a-number just less than $g/2$ which intersect but are not contained in the supersingular locus of $\mathcal{A}_g$, see Section 6.3.

1.5. Earlier work. After finishing this research, we became aware of some other results about the cohomology of Hermitian curves. In [HJ90], the authors study filtrations of the crystalline cohomology of Hermitian curves with the motivation of understanding filtrations of Weyl modules of algebraic groups. In [Dum95, Dum99], Dummigan analyzes $\mathrm{Jac}(X_q)$ viewed as a constant abelian variety over the function field of X_q. His motivation is to study the structure of the Tate-Shafarevich group Ш of $\mathrm{Jac}(X_q)$ and the determinant of the lattice $\mathrm{End}_{\mathbb{F}_{q^2}}(\mathrm{Jac}(X_q))$. In particular, he proves that Ш is trivial if and only if $n \leq 2$ and the smallest power of p annihilating Ш is $p^{\lfloor n/3 \rfloor}$. He uses the alternative equation $u^{q+1} + v^{q+1} + w^{q+1} = 0$ for X_q to find a basis for the crystalline cohomology of the lifting X_q^* of X_q over the Witt vectors which is convenient for computing the action of F. As part of [Dum95], Dummigan finds the structure of $H^1_{\mathrm{dR}}(X_q)$ as an $\mathbb{F}_{q^2}[G]$-module and as an $\mathbb{F}_p[G]$-module.

It appears that the blocks defined in Definition 4.2 are the indecomposable $\mathbb{F}_{q^2}[G]$-modules of $H^1_{\mathrm{dR}}(X_q)$. It might be possible to cut Section 3 of this paper by referring to [Dum95]. We decided to include the material in Section 3 because the method in [Dum95] relies heavily on a property of the Hermitian curve which is quite rare, namely that there is a decomposition of $H^1_{\mathrm{dR}}(X_q)$ into one-dimensional eigenspaces for a group of prime-to-p automorphisms. In contrast, the method in Section 3 involving the action of F and V on $H^1_{\mathrm{dR}}(X_q)$ can be used to compute the Ekedahl-Oort type for a wide class of Jacobians. In addition, our description of the combinatorial structure in terms of orbits of $\langle \times 2 \rangle$ may be easier to work with than the *circle diagrams* of [Dum95, Section 7].

1.6. Outline of paper. Section 2 contains background material about p-torsion group schemes and the de Rham cohomology, and some p-adic formulae. In Section 2.2, we give examples and explain the case $n = 3$ in order to give a conceptual overview of the combinatorial structures found in the paper. The action of F and V on $H^1_{\mathrm{dR}}(X_q)$ is computed in Section 3. A decomposition of $H^1_{\mathrm{dR}}(X_q)$ into blocks permuted by F and V is developed in Section 4. Section 5 contains the main theorem about the bijection between indecomposable factors of the Dieudonné module and orbits of $\langle \times 2 \rangle$. The applications are in Section 6.

The first author was partially supported by NSF grant DMS-11-01712. The second author was partially supported by NSERC and AITF. We would like to thank J. Achter, A. Hulpke, and F. Oort for helpful conversations and the referees for their valuable comments.

2. Notation and background.

2.1. Classification of p-torsion group schemes.

2.1.1. Frobenius and Verschiebung. Suppose A is a principally polarized abelian variety of dimension g defined over k. For example, A could be the Jacobian of a k-curve of genus g. Consider the multiplication-by-p morphism $[p] : A \to A$ which is a finite flat morphism of degree p^{2g}. It factors as $[p] = V \circ F$. Here $F : A \to A^{(p)}$ is the relative Frobenius morphism coming from the p-power map on the structure sheaf; it is purely inseparable of degree p^g. The Verschiebung morphism $V : A^{(p)} \to A$ is the dual of $F_{A^{\mathrm{dual}}}$.

2.1.2. The p-torsion group scheme. The *p-torsion group scheme* of A, denoted $A[p]$, is the kernel of $[p]$. It is a finite commutative group scheme annihilated by p, again having morphisms F and V. The polarization of A induces a symmetry on $A[p]$ as defined in [Oor01, 5.1]; when $p > 2$, this is an anti-symmetric isomorphism from $A[p]$ to the Cartier dual group scheme $A[p]^{\mathrm{dual}}$ of $A[p]$. By [Oor01, 9.5], the p-torsion group scheme $A[p]$ is a polarized BT_1 group scheme over k (short for polarized Barsotti-Tate truncated level 1 group scheme), as defined in [Oor01, 2.1, 9.2]. The rank of $A[p]$ is p^{2g}.

Here is a brief summary of the classification [Oor01, Theorem 9.4 &12.3] of polarized BT_1 group schemes over k in terms of Dieudonné modules and Ekedahl-Oort type; other useful references are [Kra] (unpublished - without polarization) and [Moo01] (for $p \geq 3$). When $p = 2$, there are complications with the polarization which are resolved in [Oor01, 9.2, 9.5, 12.2].

2.1.3. Covariant Dieudonné modules. One can describe the group scheme $A[p]$ using (the modulo p reduction of) the *covariant Dieudonné module*, see e.g., [Oor01, 15.3]. This is the dual of the contravariant theory found in [Dem86]. Briefly,

consider the non-commutative ring $\mathbb{E} = k[F, V]$ generated by semi-linear operators F and V with the relations $FV = VF = 0$ and $F\lambda = \lambda^p F$ and $\lambda V = V\lambda^p$ for all $\lambda \in k$. Let $\mathbb{E}(A_1, \ldots, A_r)$ denote the left ideal $\sum_{i=1}^{r} \mathbb{E}A_i$ of $\mathbb{E}$ generated by $\{A_i \mid 1 \leq i \leq r\}$. The category of commutative group schemes over k annihilated by p is equivalent to the category of finite left $\mathbb{E}$-modules. Given a BT_1 group scheme $\mathbb{G}$ over k we denote by $D(\mathbb{G})$ the Dieudonné module of $\mathbb{G}$. If $\mathbb{G}$ has rank p^{2g}, then $D(\mathbb{G})$ has dimension $2g$ as a k-vector space. For example, the Dieudonné module of a supersingular elliptic curve is $\mathbb{E}/\mathbb{E}(F + V)$, [Gor02, Ex. A.5.4].

2.1.4. The p-rank and a-number. Two invariants of (the p-torsion of) an abelian variety are the p-rank and a-number. The *p-rank* of A is $f = \dim_{\mathbb{F}_p} \mathrm{Hom}(\mu_p, A[p])$ where μ_p is the kernel of Frobenius on $\mathbb{G}_m$. Then p^f is the cardinality of $A[p](k)$. The *a-number* of A is $a = \dim_k \mathrm{Hom}(\alpha_p, A[p])$ where α_p is the kernel of Frobenius on $\mathbb{G}_a$. It is well-known that $0 \leq f \leq g$ and $1 \leq a + f \leq g$. Then A is *superspecial* if $a = g$. The p-rank of $\mathbb{G} = A[p]$ is the dimension of $V^g D(\mathbb{G})$. The a-number of $A[p]$ equals $g - \dim(V^2 D(\mathbb{G}))$ [LO98, 5.2.8].

2.1.5. The Ekedahl-Oort type. As in [Oor01, Sections 5 & 9], the isomorphism type of a BT_1 group scheme $\mathbb{G}$ over k can be encapsulated into combinatorial data. If $\mathbb{G}$ is symmetric with rank p^{2g}, then there is a *final filtration* $N_1 \subset N_2 \subset \cdots \subset N_{2g}$ of $D(\mathbb{G})$ as a k-vector space which is stable under the action of V and F^{-1} such that $i = \dim(N_i)$, [Oor01, 5.4]. If w is a word in V and F^{-1}, then $wD(\mathbb{G})$ is an object in the filtration; in particular, $N_g = VD(\mathbb{G}) = F^{-1}(0)$.

The *Ekedahl-Oort type* of $\mathbb{G}$, also called the *final type*, is $\nu = [\nu_1, \ldots, \nu_g]$ where $\nu_i = \dim(V(N_i))$. The p-rank is $\max\{i \mid \nu_i = i\}$ and the a-number equals $g - \nu_g$. The Ekedahl-Oort type of $\mathbb{G}$ does not depend on the choice of a final filtration. There is a restriction $\nu_i \leq \nu_{i+1} \leq \nu_i + 1$ on the final type. There are 2^g Ekedahl-Oort types of length g since all sequences satisfying this restriction occur. By [Oor01, 9.4, 12.3], there are bijections between (i) Ekedahl-Oort types of length g; (ii) polarized BT_1 group schemes over k of rank p^{2g}; and (iii) principal quasi-polarized Dieudonné modules of dimension $2g$ over k.

In the terminology of [EvdG09, Section 2.2], an integer $1 \leq i \leq g$ is a *break point* of ν if either $\nu_{i-1} = \nu_i \neq \nu_{i+1}$ or $\nu_{i-1} \neq \nu_i = \nu_{i+1}$. The Ekedahl-Oort type is determined by its break points, since these are the indices at which the behavior of the sequence ν_i switches between the states of being constant and increasing. The break points are the last indices of the *canonical fragments* of ν.

2.1.6. The de Rham cohomology. By [Oda69, Section 5], there is an isomorphism of $\mathbb{E}$-modules between the Dieudonné module of the p-torsion group scheme $\mathrm{Jac}(X_q)[p]$ and the de Rham cohomology group $H^1_{\mathrm{dR}}(X_q)$.

Applying [Oda69, Section 5], there is the following description of $H^1_{\mathrm{dR}}(X_q)$. Recall that $\dim_k H^1_{\mathrm{dR}}(X_q) = 2g$. Consider the open cover $\mathcal{U}$ of X_q given by $U_1 = X_q \setminus \{P_\infty\}$ and $U_2 = X_q \setminus \{(0, y) \mid y^q + y = 0\}$. For a sheaf $\mathcal{F}$ on X_q, let

$$\mathcal{C}^0(\mathcal{U}, \mathcal{F}) := \{\kappa = (\kappa_1, \kappa_2) \mid \kappa_i \in \Gamma(U_i, \mathcal{F})\},$$
$$\mathcal{C}^1(\mathcal{U}, \mathcal{F}) := \{\phi \in \Gamma(U_1 \cap U_2, \mathcal{F})\}.$$

The coboundary operator $\delta : \mathcal{C}^0(\mathcal{U}, \mathcal{F}) \to \mathcal{C}^1(\mathcal{U}, \mathcal{F})$ is defined by $\delta\kappa = \kappa_i - \kappa_j$.

The closed de Rham cocycles are defined by

$$Z^1_{\mathrm{dR}}(\mathcal{U}) := \{(\phi, \omega) \in \mathcal{C}^1(\mathcal{U}, \mathcal{O}) \times \mathcal{C}^0(\mathcal{U}, \Omega^1) \mid d\phi = \delta\omega\},$$

that is, $d\phi = \omega_1 - \omega_2$. The de Rham coboundaries are defined by

$$B^1_{\mathrm{dR}}(\mathcal{U}) := \{(\delta\kappa, d\kappa) \in Z^1_{\mathrm{dR}}(\mathcal{U}) \mid \kappa \in C^0(\mathcal{U}, \mathcal{O})\}.$$

Finally,

$$H^1_{\mathrm{dR}}(X_q) \cong H^1_{\mathrm{dR}}(X_q)(\mathcal{U}) := Z^1_{\mathrm{dR}}(\mathcal{U})/B^1_{\mathrm{dR}}(\mathcal{U}).$$

There is an injective homomorphism $\lambda : H^0(X_q, \Omega^1) \to H^1_{\mathrm{dR}}(X_q)$ denoted informally by $\omega \mapsto (0, \omega)$ where the second coordinate is defined by $\omega_i = \omega|_{U_i}$. This map is well-defined since $d(0) = \omega|_{U_1} - \omega|_{U_2} = \delta\omega$. It is injective because, if $(0, \omega) \equiv (0, \omega') \bmod B^1_{\mathrm{dR}}(\mathcal{U})$, then $\omega - \omega' = d\kappa$ where $\kappa \in C^0(\mathcal{U}, \mathcal{O})$ is such that $\delta\kappa = 0$; thus κ is a constant function on X and so $\omega - \omega' = 0$.

There is another homomorphism $\gamma : H^1_{\mathrm{dR}}(X_q) \to H^1(X_q, \mathcal{O})$ sending the cohomology class of (ϕ, ω) to the cohomology class of ϕ. The choice of cocycle (ϕ, ω) does not matter, since the coboundary conditions on $H^1_{\mathrm{dR}}(X_q)$ and $H^1(X_q, \mathcal{O})$ are compatible. The homomorphisms λ and γ fit into a short exact sequence

$$0 \to H^0(X_q, \Omega^1) \xrightarrow{\lambda} H^1_{\mathrm{dR}}(X_q) \xrightarrow{\gamma} H^1(X_q, \mathcal{O}) \to 0.$$

In Subsection 3.1, we construct a suitable section $\sigma : H^1(X_q, \mathcal{O}) \to H^1_{\mathrm{dR}}(X_q)$ of γ as k-vector spaces.

2.1.7. The action of Frobenius and Verschiebung on $H^1_{\mathrm{dR}}(X_q)$. The Frobenius and Verschiebung operators F and V act on $H^1_{\mathrm{dR}}(X_q)$ as follows:

$$F(f, \omega) := (f^p, 0) \quad \text{and} \quad V(f, \omega) := (0, \mathcal{C}(\omega)),$$

where $\mathcal{C}$ is the Cartier operator [Car57] on the sheaf Ω^1. The operator F is p-linear and V is p^{-1}-linear. In particular, $\ker(F) = H^0(X_q, \Omega^1) = \mathrm{im}(V)$.

The three principal properties of the Cartier operator are that it annihilates exact differentials, preserves logarithmic ones, and is p^{-1}-linear. The Cartier operator can be computed as follows. The element $x \in k(X_q)$ forms a p-basis of $k(X_q)$ over $k(X_q)^p$, i.e., every $z \in k(X_q)$ can be written as $z := z_0^p + z_1^p x + \cdots + z_{p-1}^p x^{p-1}$ for uniquely determined $z_0, \ldots, z_{p-1} \in k(X_q)$. Then $\mathcal{C}(z\,dx/x) := z_0\,dx/x$.

2.2. Examples and conceptual overview. We illustrate the structure of the p-torsion group schemes of the Jacobians of the Hermitian curves X_{p^n} for $n \leq 3$ as a way of motivating later computations. The case $n = 4$ can be found in Example 5.18.

The p-rank of X_q is zero since X_q is supersingular. Let $r_{n,i}$ denote the rank of the ith iterate of the Cartier operator $\mathcal{C}$ on $H^0(X_q, \Omega^1)$. The a-number of X_q is $a_n = g - r_{n,1}$. In Proposition 3.5, we prove that

$$r_{n,i} = p^n(p+1)^i(p^{n-i} - 1)/2^{i+1}.$$

2.2.1. The case $n = 1$. When $n = 1$, then the rank of $\mathcal{C}$ is $r_{1,1} = 0$ and so the a-number is $a_1 = g$. By definition, X_1 is superspecial. The Ekedahl-Oort type of $\mathrm{Jac}(X_p)[p]$ is $[0, \ldots, 0]$ and $\mathbb{D}(X_p) = (\mathbb{E}/\mathbb{E}(F + V))^g$ as in (1).

2.2.2. The case $n = 2$. When $n = 2$, then $r_{2,1} = g/2$ and $r_{2,2} = 0$. The Ekedahl-Oort type $\nu = [\nu_1, \ldots, \nu_g]$ has values $\nu_g = g/2$ and $\nu_{g/2} = 0$. By the numerical restrictions on ν found in Section 2.1.5, this implies that $\nu_i = 0$ and $\nu_{g/2+i} = i$ for $1 \leq i \leq g/2$, so that $\nu = [0, \ldots, 0, 1, 2, \ldots, g/2]$.

Using [Oor01, 9.1], the Dieudonné module is generated by variables Z_i for $1 \leq i \leq 2g$ which are defined in terms of variables Y_i and X_i for $1 \leq i \leq g$. Imprecisely speaking, the variables Y_i are used (in reverse order) for the indices where the value in the Ekedahl-Oort type stays constant, and the variables X_i are used for the indices where the value in the Ekedahl-Oort type is increasing. In the case $n = 2$, this yields:

i	$1 \leq i \leq g/2$	$1 + g/2 \leq i \leq g$	$g + 1 \leq i \leq 3g/2$	$1 + 3g/2 \leq i \leq 2g$
Z_i	Y_{g+1-i}	$X_{i-g/2}$	$Y_{1-i+3g/2}$	X_{i-g}

For $1 \leq i \leq g$, the actions of Frobenius and Verschiebung are defined by the rules:

$$F(X_i) = Z_i,\ F(Y_i) = 0,\ V(Z_i) = 0,\ V(Z_{2g+1-i}) = \pm Y_i.$$

With respect to the ordered variables $Z_1, \ldots, Z_{2g}$, the action of F and V are given by the following (each entry represents a square matrix of size $g/2$):

$$F = \begin{pmatrix} 0 & I & 0 & 0 \\ 0 & 0 & 0 & I \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},\ V = \begin{pmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -I \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Thus $\mathbb{D}(X_{p^2})$ is generated by Z_i with relation $(F^2 + V^2)Z_i = 0$ for $1 + 3g/2 \leq i \leq 2g$, proving $\mathbb{D}(X_{p^2}) = (\mathbb{E}/\mathbb{E}(F^2 + V^2))^{g/2}$ as in (2).

2.2.3. The case $n = 3$. For $n = 3$ (or larger), the information gleaned from ranks of iterates of the Cartier operator is not enough to determine the structure of the p-torsion group scheme. When $n = 3$, $\nu_g = r_{3,1}$, $\nu_{r_{3,1}} = r_{3,2}$ and $\nu_{r_{3,2}} = 0$. Since $r_{3,1} = 2r_{3,2}$, the values ν_i remain 0 for $1 \leq i \leq r_{3,2}$ and then increase by one at each index for $r_{3,2} < i \leq r_{3,1}$. Among the indices $r_{3,1} < i \leq g$, it is clear that the values ν_i must rise by a combined total of $r_{3,2}$. In other words, the value ν_i must increase at somewhat more than half of the indices i in this range, but it is not clear at which ones.

More information is required to determine the values ν_i for $r_{3,1} < i < g$, specifically, the full structure of $H^1_{\mathrm{dR}}(X_q)$ as an $\mathbb{E}$-module. We compute the actions of F and V on a basis for $H^1_{\mathrm{dR}}(X_q)$ in Section 3.3. The results are numerically intricate and it is not initially clear how to find a filtration $N_1 \subset N_2 \subset \cdots \subset N_{2g}$ of $H^1_{\mathrm{dR}}(X_q)$ which is stable under the action of V and F^{-1}.

At this stage, computer calculations for small p convinced us that the values ν_i stay as small as possible in the range $r_{3,1} < i \leq g$; in other words, that $\nu_i = r_{3,2}$ for $r_{3,1} < i \leq g - r_{3,2}$ and then ν_i increases by one at each index in the range $g - r_{3,2} < i \leq g$. We came to expect that the Ekedahl-Oort type has the break points $r_{3,2}$, $r_{3,1}$, and $g - r_{3,2}$ when $n = 3$ and considered the implications of this hypothesis.

This hypothesis implies that the interval $1 \leq i \leq 2g$ is divided into 8 canonical fragments, six of size $r_{3,2}$ and two of size $g - 3r_{3,2}$, for which the sequence ν_i switches between the states of being constant and increasing. Labeling these as $B_1, \ldots, B_8$, the technique of [Oor01, 9.1] implies that, for $1 \leq i \leq 8$,

$$F(B_i) = B_{i/2} \text{ if } i \text{ even and } F(B_i) = 0 \text{ if } i \text{ odd};$$

and, for $1 \leq i \leq 4$,

$$V(B_i) = 0 \text{ and } V(B_{4+i}) = \pm B_{2i-1}.$$

This implies that $\mathbb{D}(X_{p^3})$ is generated by the $r_{3,2}$ variables in B_8 and the $g - 3r_{3,2} = (\frac{p(p-1)}{2})^3$ variables in B_6, subject to the relations that $F^3 + V^3 = 0$ on B_8 and $F + V = 0$ on B_6. On each block B_i, exactly one of F^{-1} and V is defined, and the action on the blocks is the same as $\langle \times 2 \rangle$ on $\mathbb{Z}/9 - \{0\}$.

To prove this, we find a decomposition of $H^1_{\mathrm{dR}}(X_q)$ into blocks B_i, which is compatible with the condition that the final filtration must be a refinement of the filtration:

$$0 = T_0 \subset T_1 \subset T_2 \subset \cdots \subset T_8,$$

where

i	1	2	3	4	5	6	7	8
T_i/T_{i-1}	B_1	B_5	B_3	B_7	B_2	B_6	B_4	B_8

.

For example, this shows $H^0(X_q, \Omega^1) = \mathrm{Span}(B_1, B_3, B_5, B_7)$ and $H^1(X_q, \mathcal{O}) = \mathrm{Span}(B_2, B_4, B_6, B_8)$.

We assign basis vectors of $H^0(X_q, \Omega^1)$ and $H^1(X_q, \mathcal{O})$ to blocks based on the following rules, see Sections 4.1 and 4.2. Given $i, j \geq 0$ such that $i + j \leq p^3 - 2$, consider the p-adic expansions $i = i_0 + i_1 p + i_2 p^2$ and $j = j_0 + j_1 p + j_2 p^2$. Define $b_0, b_1 \in \mathbb{Z}/2$ by $b_0 = 0$ iff $i_0 + j_0 < p - 1$ and $b_1 = 0$ iff $i_0 + i_1 p + j_0 + j_1 p < p^2 - 1$. To a basis vector $\omega_{i,j} = x^i y^j dx$ of $H^0(X_q, \Omega^1)$, we assign the vector $(b_0, b_1, 1) \in (\mathbb{Z}/2)^3$. To a basis vector $f_{i,j} = \frac{1}{x^i y^j} \frac{y^{q-1}}{x}$ of $H^1(X_q, \mathcal{O})$, we assign the vector $(b_0, b_1, 0) \in (\mathbb{Z}/2)^3$. We then assign the vectors to blocks by:

$H^1(X_q, \mathcal{O})$

vector	$(0,0,0)$	$(0,1,0)$	$(1,0,0)$	$(1,1,0)$
block	B_8	B_6	B_4	B_2

,

and

$H^0(X_q, \Omega^1)$

vector	$(0,0,1)$	$(0,1,1)$	$(1,0,1)$	$(1,1,1)$
block	B_1	B_3	B_5	B_7

.

We conclude (and prove in Theorem 5.13) that the Dieudonné module of $\mathrm{Jac}(X_{p^3})[p]$ is:

$$\mathbb{D}(X_{p^3}) = (\mathbb{E}/\mathbb{E}(F^3 + V^3))^{r_{3,2}} \oplus (\mathbb{E}/\mathbb{E}(F + V))^{g - 3r_{3,2}}. \tag{3}$$

2.2.4. The case $n = 4$. See Example 5.18 for the structure of the Dieudonné module when $n = 4$.

2.2.5. Strategy for general n. For larger values of n we follow a similar strategy. We find a basis of $H^1_{\mathrm{dR}}(X_q)$ using a basis of regular 1-forms $\omega_{i,j} = x^i y^j \, dx$ for $H^0(X_q, \Omega^1)$ and a basis of functions $f_{i,j} = \frac{1}{x^i y^j} \frac{y^{q-1}}{x}$ for $H^1(X_q, \mathcal{O})$. We compute the image of F and V on $H^1_{\mathrm{dR}}(X_q)$ and form blocks spanned by basis vectors which have the same behavior under iterates of F and V. On each block, either F acts bijectively and V as the zero operator, or vice-versa. The structure of the Dieudonné module of X_q is determined by the (generalized) permutation of the blocks under F and V.

To provide some intuition for the main result, Theorem 5.13, we discuss in non-precise terms how this structure is related to multiplication-by-2 on $\mathbb{Z}/(2^n + 1)$. As in the $n = 3$ case, the behavior of F and V is determined by the p-adic expansions

of i and j, specifically whether or not the base-p sum of i and j 'carries' in the k-th digit for $0 \le k < n$. This allows us to index the blocks by binary vectors in $(\mathbb{Z}/2)^n$. Since Frobenius acts by multiplication-by-p on exponents, it acts like a 'shift' on the base-p digits of i and j, and thus by a 'shift' on the binary vectors.

We re-index the blocks by non-zero elements of $\mathbb{Z}/(2^n+1)$. Exactly one of F^{-1} and V acts bijectively on each block; it acts like multiplication-by-2 on the index. In the rest of the paper, we make this description precise, thus giving an explicit one-to-one correspondence between the distinct indecomposable factors of the Dieudonné module of X_q and the orbits of $\langle \times 2 \rangle$ on $\mathbb{Z}/(2^n+1) - \{0\}$.

2.3. Some p-adic formulae. Given a positive integer $m < p^n$, we fix some notation. For $0 \le h \le n-1$, let $m_h \in \{0, 1, \dots, p-1\}$ be the hth coefficient in the p-adic expansion of m:

$$m = m_0 + m_1 p + \cdots + m_{n-1} p^{n-1}.$$

For $1 \le h \le n$, let

$$m_h^+ := \sum_{l=0}^{h-1} m_l p^l \text{ and } m_h^T := \sum_{l=1}^{h-1} m_l p^{l-1}.$$

Note that $m = m_0 + p m_n^T$ and $m = m_{n-1} p^{n-1} + m_{n-1}^+$ with $0 \le m_n^T, m_{n-1}^+ \le p^{n-1} - 1$. Also

$$m_h^+ = m_0 + p m_h^T. \tag{4}$$

The following lemma will be useful in the proof of Proposition 4.7.

LEMMA 2.1. *Suppose* $1 \le i, j \le p^n$.

1. *If* $i_h^T + j_h^T < p^h - 1$ *then* $i_{h+1}^+ + j_{h+1}^+ < p^{h+1} - 1$ *and the converse is true if* $i_0 + j_0 \ge p - 1$.
2. *If* $i_{h+1}^+ + j_{h+1}^+ < p^{h+1} - 1$ *then* $(p^h - 1 - i_h^T) + (p^h - 1 - j_h^T) \ge p^h - 1$ *and the converse is true if* $i_0 + j_0 < p - 1$.
3. *Also:* $i_h^+ + j_h^+ < p^h - 1$ *if and only if* $p - 1 + j_{n-1} + p(i_h^+ + j_h^+) < p^{h+1} - 1$.
4. *Also:* $i_h^+ + j_h^+ < p^h - 1$ *if and only if* $2p^{h+1} - 2 - (i_h^+ + j_h^+)p - p - j_{n-1} \ge p^{h+1} - 1$.

Proof.

1. The condition $i_{h+1}^+ + j_{h+1}^+ < p^{h+1} - 1$ is equivalent to the condition $(i_h^T + j_h^T)p < p^{h+1} - (i_0 + j_0 + 1)$. The result follows since $i_0 + j_0 + 1 \le 2p - 1$ and, under the given condition, $i_0 + j_0 + 1 \ge p$.
2. The condition $i_{h+1}^+ + j_{h+1}^+ < p^{h+1} - 1$ is equivalent to the condition $(i_h^T + j_h^T)p < p^{h+1} - (i_0 + j_0 + 1)/p$. Using the bounds $1 \le i_0 + j_0 + 1$ and, under the given condition, $i_0 + j_0 + 1 < p$, this condition is equivalent to $i_h^T + j_h^T \le p^h - 1$, which is equivalent to the condition $(p^h - 1 - i_h^T) + (p^h - 1 - j_h^T) \ge p^h - 1$.
3. This follows from the facts that $p(i_h^+ + j_h^+) \le p^{h+1} - 2p$ when $i_h^+ + j_h^+ < p^h - 1$ and $p(i_h^+ + j_h^+) \ge p^{h+1} - p$ when $i_h^+ + j_h^+ \ge p^h - 1$ and $0 \le j_{n-1} \le p - 1$.
4. Similar to part (3).

∎

3. The de Rham cohomology of Hermitian curves. In this section, we compute the actions of F and V with respect to a chosen basis for $H^1_{\mathrm{dR}}(X_q)$. An essential point is that these actions are scaled permutation matrices with respect to this basis, see Corollary 3.3.

3.1. A basis for the de Rham cohomology. Consider the following set of lattice points of the plane:

$$\Delta := \{(i,j) \mid i,j \in \mathbb{Z},\ i,j \geq 0,\ i+j \leq q-2\}.$$

On the Hermitian curve $X_q : y^q + y = x^{q+1}$, the functions x and y have poles at P_∞, with $v_{P_\infty}(x) = -q$ and $v_{P_\infty}(y) = -(q+1)$. Note that $(i,j) \in \Delta$ if and only if $i,j \geq 0$ and $iq + j(q+1) \leq 2g-2$.

LEMMA 3.1. *A basis for $H^0(X_q, \Omega^1)$ is given by the set*

$$\mathbb{B}_0 := \{\omega_{i,j} := x^i y^j\, dx \mid (i,j) \in \Delta\}.$$

Proof. This is a special case of [Sul75, Lemma 1]. □

LEMMA 3.2. *A basis for $H^1(X_q, \mathcal{O})$ is given by the set*

$$\mathbb{B}_1 := \left\{ f_{i,j} := \frac{1}{x^i y^j} \frac{y^{q-1}}{x} \mid (i,j) \in \Delta \right\}.$$

Proof. To compute $H^1(X_q, \mathcal{O})$, consider the open cover $\mathcal{U}$ of X_q given by $U_1 = X_q \setminus \{P_\infty\}$ and $U_2 = X_q \setminus \{(0,y) \mid y^q + y = 0\}$. For $i,j \in \mathbb{Z}$, consider the functions $f_{i,j} \in \Gamma(U_1 \cap U_2, \mathcal{O})$. If $0 \leq j \leq q-1$, the valuation of $f_{i,j}$ at P_∞ is:

$$v_\infty(f_{i,j}) = -(q+1)(q-1-j) + q(i+1) = j(q+1) + iq - (q^2+q-1).$$

If also $i + j \leq q-2$, then $v_\infty(f_{i,j}) < 0$ and so $f_{i,j} \notin \Gamma(U_2, \mathcal{O})$. If also $i \geq 0$, then $f_{i,j}$ has poles above $x = 0$ and so $f_{i,j} \notin \Gamma(U_1, \mathcal{O})$. Thus (the equivalence class of) the function $f_{i,j}$ is non-zero in $H^1(X_q, \mathcal{O})$ if $i,j \geq 0$ and $i + j \leq q-2$. These functions $f_{i,j}$ are linearly independent in $H^1(X_q, \mathcal{O})$ since their pole orders at P_∞ are different. They form a basis for $H^1(X_q, \mathcal{O})$ because there are g pairs (i,j) satisfying these conditions. □

Given $f \in \mathcal{O}$, it is possible to write $df = \omega(f)_1 + \omega(f)_2$ where $\omega(f)_i \in \Gamma(U_i, \Omega^1)$. Let $\tilde{f}_{i,j} = (f_{i,j}, \omega(f_{i,j})_1, \omega(f_{i,j})_2)$ denote the image of $f_{i,j}$ in $H^1_{\mathrm{dR}}(X_q)$.

In the rest of this section, we prove that this basis is convenient for computing the actions of F and V.

COROLLARY 3.3. *With respect to the basis $\mathbb{B} = \mathbb{B}_0 \cup \mathbb{B}_1$, the actions of V and F on $H^1_{\mathrm{dR}}(X_q)$ are scaled permutation matrices, i.e., they have at most one non-zero entry in each row and each column.*

Proof. This follows from Lemma 3.4, Proposition 3.6 and Proposition 3.7. □

3.2. The action of V on $H^0(X_q, \Omega^1)$.

LEMMA 3.4. *For $(i,j) \in \Delta$, write $i := i_0 + p i_n^T$ and $j := j_0 + p j_n^T$ with $0 \leq i_0, j_0 \leq p-1$ and $0 \leq i_n^T, j_n^T \leq p^{n-1} - 1$. There is a constant $d'_{i,j} \neq 0$ such that the action of V on $\omega_{i,j} \in H^0(X_q, \Omega^1)$ is given by:*

$$V(\omega_{i,j}) = \begin{cases} 0 & \text{if } i_0 + j_0 < p-1, \\ d'_{ij} \omega_{p^{n-1}(p-1-i_0)+i_n^T,\, p^{n-1}(i_0+j_0-(p-1))+j_n^T} & \text{if } i_0 + j_0 \geq p-1. \end{cases}$$

Proof. It suffices to computing the image of the Cartier operator $\mathcal{C}$ on $\omega_{i,j}$:

$$\begin{aligned}\mathcal{C}(x^i y^j\,dx) &= x^{i_n^T} y^{j_n^T}\,\mathcal{C}\left(x^{i_0}(x^{q+1}-y^q)^{j_0}\,dx\right)\\ &= x^{i_n^T} y^{j_n^T}\sum_{l=0}^{j_0}\binom{j_0}{l}(-1)^l\,\mathcal{C}\left(x^{(q+1)(j_0-l)}y^{ql}x^{i_0}\,dx\right)\\ &= x^{i_n^T} y^{j_n^T}\sum_{l=0}^{j_0}\binom{j_0}{l}(-1)^l x^{p^{n-1}(j_0-l)}y^{p^{n-1}l}\,\mathcal{C}\left(x^{i_0+j_0-l}\,dx\right).\end{aligned}$$

Now $\mathcal{C}(x^k\,dx)\neq 0$ if and only if $k\equiv -1 \bmod p$. The exponent of x satisfies

$$0\leq i_0+j_0-l\leq 2p-2.$$

The value congruent to $-1 \mod p$ in this interval is $i_0+j_0-l=p-1$. Thus $V(\omega_{i,j})=0$ unless $i_0+j_0\geq p-1$. If this is the case then substituting $l=i_0+j_0-(p-1)$ gives the desired result where

$$d'_{ij}=\binom{j_0}{i_0+j_0-(p-1)}(-1)^{i_0+j_0-(p-1)}.$$

□

Let $r_{n,i}$ denote the rank of the ith iterate of the Cartier operator on $H^0(X_q,\Omega^1)$ and let a_n be the a-number of $\mathrm{Jac}(X_q)$. The value of a_n was previously computed in [Gro90, Proposition 14.10].

Proposition 3.5.

1. *The rank $r_{n,i}$ of $\mathcal{C}^i$ on $H^0(X_q,\Omega^1)$ is*
$$r_{n,i}=p^n(p+1)^i(p^{n-i}-1)/2^{i+1}.$$
2. *The a-number a_n of $\mathrm{Jac}(X_q)$ is*
$$a_n=p^n(p^{n-1}+1)(p-1)/4.$$

Proof. Note that $\omega_{i,j}\in\mathrm{Ker}(\mathcal{C})$ iff $i_0+j_0<p-1$. More generally, $\omega_{i,j}\in\mathrm{Ker}(\mathcal{C}^r)-\mathrm{Ker}(\mathcal{C}^{r-1})$ if and only if:

$$i_0+j_0\geq p-1,\ i_1+j_1\geq p-1,\ldots,i_{r-2}+j_{r-2}\geq p-1,\ i_{r-1}+j_{r-1}<p-1.$$

This proves the first item. The second item follows since $a_n=g-r_{n,1}$. □

3.3. The action of F and V on an image of $H^1(X_q,\mathcal{O})$ in $H^1_{\mathrm{dR}}(X_q)$.

3.3.1. The Action of Frobenius.

Proposition 3.6. *For $(i,j)\in\Delta$, write $i=i_{n-1}p^{n-1}+i^+_{n-1}$ and $j=j_{n-1}p^{n-1}+j^+_{n-1}$ with $0\leq i_{n-1},j_{n-1}\leq p-1$ and $0\leq i^+_{n-1},j^+_{n-1}\leq p^{n-1}-1$. Say Case A means that $i^+_{n-1}+j^+_{n-1}<p^{n-1}-1$ and Case B means that $i^+_{n-1}+j^+_{n-1}\geq p^{n-1}-1$. There are constants $c_{i,j},d_{i,j}\neq 0$ such that the action of F on $\tilde{f}_{i,j}\in H^1_{\mathrm{dR}}(X_q)$ is given by:*

$$F\left(\tilde{f}_{i,j}\right)=\begin{cases}c_{ij}f_{pi^+_{n-1}+(p-1)-i_{n-1},pj^+_{n-1}+j_{n-1}+i_{n-1}} & \text{Case } A\\ d_{ij}\omega_{(q-1)-(pi^+_{n-1}+(p-1)-i_{n-1}),q-1-(pj^+_{n-1}+j_{n-1}+i_{n-1}+1)} & \text{Case } B.\end{cases}$$

Proof. First,

$$F(f_{i,j}) = \frac{1}{y^{j_{n-1}p^n + j_{n-1}^+ p} x^{i_{n-1}p^n + i_{n-1}^+ p}} \frac{y^{qp-p}}{x^p}$$
$$= \frac{1}{y^{(j_{n-1}^+ + 1)p} x^{(i_{n-1}^+ + 1)p}} \frac{y^{q-1}}{x} \left(y^{q(p-1-j_{n-1})} y x^{-i_{n-1}q+1} \right).$$

Let $c_l = (-1)^l \binom{p-1-j_{n-1}}{l}$, then

$$y^{q(p-1-j_{n-1})} y x^{-i_{n-1}q+1} = \sum_{l=0}^{p-1-j_{n-1}} c_l x^{(q+1)(p-1-j_{n-1}-l)} y^{l+1} x^{-i_{n-1}q+1}.$$

The sum is a linear combination $\sum c_l M_l$ for $0 \le l \le p-1-j_{n-1}$ where

$$M_l = x^{q(p-1-j_{n-1}-i_{n-1}-l)} y^{l+1} x^{p-j_{n-1}-l} \text{ and } c_l = (-1)^l \binom{p-1-j_{n-1}}{l}.$$

For $l \in I_1 = \{0, \ldots, p-2-j_{n-1}-i_{n-1}\}$, the only pole of M_l is at P_∞; then $\sigma_1 := \sum_{l \in I_1} c_l M_1 \in \Gamma(U_1, \mathcal{O})$. For $l \in I_2 = \{p-j_{n-1}-i_{n-1}, \ldots, p-1-j_{n-1}\}$, the only poles of M_l are above 0; then $\sigma_2 := \sum_{l \in I_2} c_l M_1 \in \Gamma(U_2, \mathcal{O})$.

Fix $l^* = p-1-j_{n-1}-i_{n-1}$ and consider the non-zero constants $c_{i,j} := c_{l^*}$ and $d_{i,j} := -(j_{n-1}+i_{n-1}+1)c_{l^*}$. Let

$$\sigma^* := \frac{1}{y^{(j_{n-1}^+ + 1)p} x^{(i_{n-1}^+ + 1)p}} \frac{y^{q-1}}{x} M_{l^*} = \frac{c_{i,j}}{y^{pj_{n-1}^+ + j_{n-1} + i_{n-1}} x^{pi_{n-1}^+ + p - 1 - i_{n-1}}} \frac{y^{q-1}}{x}.$$

Consider

$$\omega(\sigma^*)_1 := c_{i,j} i_{n-1}^+ y^{q-1-j_{n-2}^+ p - j_{n-1} - i_{n-1}} x^{-pi_{n-1}^+ - p - 3 + i_{n-1}} \, dx,$$

and

$$\omega(\sigma^*)_2 := d_{i,j} y^{q-1-j_{n-1}^+ p - j_{n-1} - i_{n-1} - 1} x^{q-1-pi_{n-1}^+ - p - 1 + i_{n-1}} \, dx.$$

One can check that $\omega(\sigma^*)_i \in \Gamma(U_i, \Omega^1)$ and that $d(\sigma^*) = \omega(\sigma^*)_1 + \omega(\sigma^*)_2$. Thus $F(\tilde{f}_{i,j}) \equiv (\sigma^*, \omega(\sigma^*)_1, \omega(\sigma^*)_2)$ in $H^1_{\mathrm{dR}}(X_q)$. In Case A, then $(j_{n-1}^+ p + j_{n-1} + i_{n-1}) + (pi_{n-1}^+ + p - 1 - i_{n-1}) < q-1$. In this case, $d(\sigma_1) = -\omega(\sigma^*)_1$ and $d(\sigma_2) = -\omega(\sigma^*)_2$. Taking the quotient by σ_1 and σ_2 yields that

$$F\left(\tilde{f}_{i,j}\right) = c_{i,j} f_{pi_{n-1}^+ + (p-1) - i_{n-1}, pj_{n-1}^+ + j_{n-1} + i_{n-1}}.$$

In Case B, then $\omega(\sigma^*)_1$ is regular. In this case, $d(\sigma_2 + \sigma^*) = \omega(\sigma^*)_1 = -d(\sigma_2)$. Taking the quotient by σ_1 and $\sigma^* + \sigma_2$ yields that

$$F\left(\tilde{f}_{i,j}\right) = d_{i,j} \omega_{(q-1)-(pi_{n-1}^+ + (p-1) - i_{n-1}), q-1-(pj_{n-1}^+ + j_{n-1} + i_{n-1} + 1)}.$$

□

3.3.2. The Action of Verschiebung.

PROPOSITION 3.7. *For $(i,j) \in \Delta$, write $i = i_0 + i_n^T p$ and $j = j_0 + j_n^T p$ with $0 \le i_0, j_0 \le p-1$ and $0 \le i_n^T, j_n^T \le p^{n-1}-1$. Let $i^* = p^{n-1}i_0 + (p^{n-1}-1-i_n^T)$ and $j^* = p^{n-1}(p-2-i_0-j_0) + (p^{n-1}-1-j_n^T)$. There is a constant $c'_{i,j} \neq 0$ such that the action of V on $\tilde{f}_{i,j} \in H^1_{\mathrm{dR}}(X_q)$ is given by:*

$$V\left(\tilde{f}_{i,j}\right) = \begin{cases} c'_{i,j}\omega_{i^*,j^*} & \text{if } i_0+j_0 < p-1 \\ 0 & \text{if } i_0+j_0 \ge p-1. \end{cases}$$

Proof. Let

$$\omega(f_{i,j})_1 = -(i+1)y^{q-j-1}x^{-i-2}\,dx \text{ and } \omega(f_{i,j})_2 = -(j+1)y^{q-j-2}x^{-i-1}\,dy$$

One can check that $\omega(f_{i,j})_1 \in \Gamma(U_1, \Omega^1)$ and $\omega(f_{i,j})_2 \in \Gamma(U_2, \Omega^1)$ and that $df_{i,j} = \omega(f_{i,j})_1 + \omega(f_{i,j})_2$.

Recall that $V(f,\omega) := (0, \mathcal{C}(\omega))$. Since $\mathcal{C}(\omega(f_{i,j})_1) + \mathcal{C}(\omega(f_{i,j})_2) = 0$, it is only necessary to compute $\mathcal{C}(-\omega(f_{i,j})_1)$ which equals

$$\mathcal{C}\left((i+1)y^{q-j-1}x^{-i-2}\,dx\right) = (i_0+1)y^{q/p-j_n^T-1}x^{-i_n^T}\,\mathcal{C}\left(y^{p-j_0-1}x^{-i_0-2}\,dx\right).$$

Now, $\mathcal{C}\left(y^{p-j_0-1}x^{-i_0-2}\,dx\right) = \mathcal{C}\left(\left(x^{q+1}-y^q\right)^{p-j_0-1}x^{-i_0-2}\,dx\right)$ which equals

$$\sum_{l=0}^{p-1-j_0}\binom{p-1-j_0}{l}\mathcal{C}\left(x^{(q+1)(p-1-j_0-l)}(-y)^{ql}x^{-i_0-2}\,dx\right).$$

Note that

$$\mathcal{C}\left(x^{(q+1)(p-1-j_0-l)}(-y)^{ql}x^{-i_0-2}\,dx\right) = (-1)^l x^{p^{n-1}(p-1-j_0-l)}y^{p^{n-1}l}\,\mathcal{C}\left(x^{p-3-j_0-i_0-l}\,dx\right).$$

The exponent $e = p-3-j_0-i_0-l$ of x satisfies

$$-p-1 \le -i_0-2 = p-3-j_0-i_0-(p-1-j_0) \le e \le p-3.$$

Recall that $\mathcal{C}(x^e\,dx) \neq 0$ if and only if $e \equiv -1 \bmod p$. Note that $e = -p-1$ only when $i_0 = p-1$, in which case the term is trivialized by $\mathcal{C}$ as seen above. As such, the only term which is not trivialized by $\mathcal{C}$ is when $e = -1$, i.e., when

$$l = p-2-i_0-j_0.$$

Thus $V(\tilde{f}_{i,j}) = 0$ if $i_0+j_0 \ge p-1$. If $i_0+j_0 \le p-2$, the claimed result follows by substituting $l = p-2-i_0-j_0$ and using the non-zero constant

$$c'_{i,j} = (i_0+1)\binom{p-1-j_0}{p-2-j_0-i_0}(-1)^{p-2-i_0-j_0}.$$

∎

4. Decomposition of the de Rham cohomology of Hermitian curves. This is the main result of this section:

COROLLARY 4.1. *There is a decomposition* $H^1_{\mathrm{dR}}(X_q) = \oplus_{1\le t\le 2^n} B_t$ *such that the morphisms* V *and* F^{-1} *act on the blocks* B_t *by multiplication-by-2 on the indices modulo* 2^n+1 *as follows.*

If $2^{n-1}+1 \le t \le 2^n$, *then there is an isomorphism* $V : B_t \to B_{2t \bmod 2^n+1}$.

If $1 \le t \le 2^{n-1}$, *then* $B_t \subset \ker(V) = \mathrm{Im}(F)$ *and there is an isomorphism* $F^{-1} : B_t \to B_{2t}$.

In order to prove this, we partition the basis $\mathbb{B} = \mathbb{B}_0 \cup \mathbb{B}_1$ for $H^1_{\mathrm{dR}}(X_q)$ into 2^n sets which are well-suited for studying the action of F and V. The sets are first indexed by vectors $\vec{b} \in (\mathbb{Z}/2)^n$ and then by non-zero $t \in \mathbb{Z}/(2^n+1)$.

4.1. A binary vector decomposition. Given $i, j \ge 0$ such that $0 \le i+j \le q-2$, recall the definitions of $i_k^+, j_k^+, i_k^T, j_k^T$ from Section 2.3. For $0 \le h \le n-2$, let

$$b_h(i,j) = \begin{cases} 0 & \text{if } i_{h+1}^+ + j_{h+1}^+ < p^{h+1}-1, \\ 1 & \text{otherwise.} \end{cases}$$

For example, $b_0(i,j) = 0$ when $i_0 + j_0 < p-1$ and $b_1(i,j) = 0$ when $i_0 + i_1 p + j_0 + j_1 p < p^2 - 1$.

DEFINITION 4.2. For each element of the basis $\mathbb{B}$ for $H^1_{\mathrm{dR}}(X_q)$, define a vector $\vec{b} = (b_0, \ldots, b_{n-1}) \in (\mathbb{Z}/2)^n$ as follows: If $\tilde{f}_{i,j} \in \mathbb{B} \cap H^1(X_q, \mathcal{O})$, let $b_{n-1}(i,j) = 0$ and

$$\vec{b}(\tilde{f}_{i,j}) = (b_0(i,j), \ldots, b_{n-2}(i,j), 0).$$

If $\omega_{i,j} \in \mathbb{B} \cap H^0(X_q, \Omega^1)$, let $b_{n-1}(i,j) = 1$ and

$$\vec{b}(\omega_{i,j}) = (b_0(i,j), \ldots, b_{n-2}(i,j), 1).$$

Finally, for $\vec{b} \in (\mathbb{Z}/2)^n$, consider the subspace

$$H^1_{\mathrm{dR}}(X_q)_{\vec{b}} := \mathrm{Span}\{\lambda \in \mathbb{B} \;\mid\; \vec{\lambda} = \vec{b}\}.$$

For notational purposes, let $H^1_{\mathrm{dR}}(X_q)_0 = 0$.

LEMMA 4.3. *Given a vector* $\vec{b} = (b_0, \ldots, b_{n-1}) \in (\mathbb{Z}/2)^n$, *let* n_s *(resp.* n_d*) be the number of adjacent terms of* $(b_0, \ldots, b_{n-2})$ *which are equal (resp. different). Then*

$$\dim(H^1_{\mathrm{dR}}(X_q)_{\vec{b}}) = \left(\frac{p(p+1)}{2}\right)^{n_s+1+b_0-b_{n-2}} \left(\frac{p(p-1)}{2}\right)^{n_d+1+b_{n-2}-b_0}.$$

Proof. The values $b_k(i,j)$ are determined by the behavior of the base-p expansion of the sum $i+j+1$. Namely, $b_k(i,j) = 1$ if and only if the sum $i+j+1$ 'carries' in the k-th digit. Since $i+j < q-1$, there is no 'carrying' out of the last digit; the addition of 1 can be thought of as 'carrying' into the first digit. Then $\dim(H^1_{\mathrm{dR}}(X_q)_{\vec{b}})$ is the number of pairs (i,j) satisfying the 'carrying pattern' associated to $\vec{b}$. It equals the product of the numbers α_k of pairs of p-adic digits (i_k, j_k) as $0 \le k \le n-1$, where $\alpha_k = \#\{(i_k, j_k) \mid 0 \le i_k, j_k \le p-1,\ i_k + j_k \le p-1-|b_k - b_{k-1}|\}$. □

4.2. A congruence decomposition. To index blocks with integers instead of binary vectors, consider this bijection $T : (\mathbb{Z}/2)^n \to \mathbb{Z}/(2^n+1) - \{0\}$.

DEFINITION 4.4. Given $\vec{b} = (b_0, \ldots, b_{n-1}) \in (\mathbb{Z}/2)^n$:
1. if $b_{n-1} = 1$, let $T(\vec{b}) = 2^{n-1}b_0 + \cdots 2b_{n-2} + 1$;
2. if $b_{n-1} = 0$, let $T(\vec{b}) = 2^n - (2^{n-1}b_0 + \cdots 2b_{n-2})$.

When r is even (resp. odd), the coordinates of the vector $T^{-1}(r)$ are the coefficients of the binary expansion of r (resp. written in reverse order).

4.3. Block structure. Consider the decomposition $H^1_{\mathrm{dR}}(X_q) = \oplus_{1 \le t \le 2^n} B_t$ where $B_t := \mathrm{Span}\{\lambda \in \mathbb{B} \mid T(\vec{\lambda}) = t\}$ for $1 \le t \le 2^n$. Corollary 4.1 is an immediate consequence of the next result.

THEOREM 4.5. *The actions of V and F on $H^1_{\mathrm{dR}}(X_q)$ satisfy the following:*
1. *if $1 \le t \le 2^{n-1}$, then $V(B_t) = 0$;*
2. *if $2^{n-1} + 1 \le t \le 2^n$, then there is an isomorphism $V|_{B_t} : B_t \to B_{2t-2^n-1}$;*
3. *if t is odd, then $F(B_t) = 0$;*
4. *if t is even, then there is an isomorphism $F|_{B_t} : B_t \to B_{t/2}$.*

The proof of Theorem 4.5 occupies the rest of the section.

4.4. The action of F and V in terms of binary vectors. In this section, we show that F and V act on $H^1_{\mathrm{dR}}(X_q)$ by permuting the subspaces $H^1_{\mathrm{dR}}(X_q)_{\vec{b}}$ for $\vec{b} \in (\mathbb{Z}/2)^n$. The next definition summarizes the change in the binary vector under the action of F and V.

DEFINITION 4.6. Let ι be the transposition $(0,1)$. Given $\vec{b} = (b_0, \ldots, b_{n-1})$, define $\vec{V}b$ and $\vec{F}b$ as follows:
1. Action of V on $H^0(X_q, \Omega^1)$: If $b_{n-1} = 1$ and $b_0 = 0$, let $\vec{V}b = 0$.
   If $b_{n-1} = 1$ and $b_0 = 1$, let $\vec{V}b = (b_1, \ldots, b_{n-2}, 0, 1)$, *(left shift with flip in last two positions).*
2. Action of V on $H^1(X_q, \mathcal{O})$: If $b_{n-1} = 0$ and $b_0 = 1$, let $\vec{V}b = 0$.
   If $b_{n-1} = 0$ and $b_0 = 0$, let $\vec{V}b = (\iota(b_1), \ldots, \iota(b_{n-2}), 1, 1)$, *(left shift with flip in all positions).*
3. Action of F on $H^0(X_q, \Omega^1)$: If $b_{n-1} = 1$, let $\vec{F}b = 0$.
4. Action of F on $H^1(X_q, \mathcal{O})$:
   [A] If $b_{n-1} = 0$ and $b_{n-2} = 0$, let $\vec{F}b = (1, b_0, \ldots, b_{n-3}, 0)$, *(right shift with flip in first position).*
   [B] If $b_{n-1} = 0$ and $b_{n-2} = 1$, let $\vec{F}b = (0, \iota(b_0), \ldots, \iota(b_{n-3}), 1)$, *(right shift with flip in all interior positions).*

PROPOSITION 4.7. *For each binary vector $\vec{b} \in (\mathbb{Z}/2)^n$:*

$$VH^1_{\mathrm{dR}}(X_q)_{\vec{b}} \cong H^1_{\mathrm{dR}}(X_q)_{\vec{V}b} \text{ and } FH^1_{\mathrm{dR}}(X_q)_{\vec{b}} \cong H^1_{\mathrm{dR}}(X_q)_{\vec{F}b}.$$

Proof. The proof that the image of F or V is in the claimed block is divided into cases as in Definition 4.6.
1. Action of V on $H^0(X_q, \Omega^1)$: If $\omega_{i,j} \in H^1_{\mathrm{dR}}(X_q)_{\vec{b}}$, the claim is that $V(\omega_{i,j}) \in H^1_{\mathrm{dR}}(X_q)_{\vec{V}b}$. Note that $b_{n-1}(\omega_{i,j}) = 1$ by definition. If $b_0(\omega_{i,j}) = 0$ then $V(\omega_{i,j}) = 0$ by Lemma 3.4.

Suppose $b_0(\omega_{i,j}) = 1$, i.e., $i_0 + j_0 \geq p-1$. By Definition 4.6(1), it suffices to show that $b_{k-1}(V(\omega_{i,j})) = b_k(\omega_{i,j})$ for $k \in \{1 \dots n-1\}$. By definition, $b_k(\omega_{i,j}) = 0$ if and only if $i^+_{k+1} + j^+_{k+1} < p^{k+1} - 1$. By Lemma 2.1(1), since $i_0 + j_0 \geq p-1$, this is equivalent to $i^T_k + j^T_k < p^k - 1$. By Lemma 3.4, this is equivalent to $b_{k-1}(V(\omega_{i,j})) = 0$. In particular, $b_{n-2}(V(\omega_{i,j})) = 0$ since $i + j < p^n - 1$.

2. Action of V on $H^1(X_q, \mathcal{O})$: If $\tilde{f}_{i,j} \in H^1_{\mathrm{dR}}(X_q)_{\vec{b}}$, the claim is that $V(\tilde{f}_{i,j}) \in H^1_{\mathrm{dR}}(X_q)_{\vec{V}b}$. Note that $b_{n-1}(\tilde{f}_{i,j}) = 0$ by definition. If $b_0(\tilde{f}_{i,j}) = 1$ then $V(\tilde{f}_{i,j}) = 0$ by Proposition 3.7.
   Suppose $b_0(\tilde{f}_{i,j}) = 0$, i.e., $i_0 + j_0 < p-1$. By Definition 4.6(2), it suffices to show $b_k(\tilde{f}_{i,j}) = 0$ if and only if $b_{k-1}(V(\tilde{f}_{i,j})) = 1$ for $1 \leq k \leq n-1$. By definition, $b_h(\tilde{f}_{i,j}) = 0$ means that $i^+_{h+1} + j^+_{h+1} < p^{h+1} - 1$. By Lemma 2.1(2), this is equivalent to $(p^k - 1 - i^T_k) + (p^k - 1 - j^T_k) \geq p^k - 1$. This is equivalent to $b_{k-1}(V(\tilde{f}_{i,j})) = 1$ by Proposition 3.7. In particular, $b_{n-2}(V(\tilde{f}_{i,j})) = 1$ since $b_{n-1}(\tilde{f}_{i,j}) = 0$.
3. Action of F on $H^0(X_q, \Omega^1)$: If $\omega_{i,j} \in H^1_{\mathrm{dR}}(X_q)_{\vec{b}}$, then $F(\omega_{i,j}) = 0$ by Section 2.1.7
4. Action of F on $H^1(X_q, \mathcal{O})$:
   For [A], given $\tilde{f}_{i,j} \in H^1_{\mathrm{dR}}(X_q)_{\vec{b}}$ such that $F(\tilde{f}_{i,j}) \in H^1(X_q, \mathcal{O})$, the claim is that $F(\tilde{f}_{i,j}) \in H^1_{\mathrm{dR}}(X_q)_{\vec{F}b}$. By Proposition 3.6, $F(\tilde{f}_{i,j}) \in H^1(X_q, \mathcal{O})$ when $b_{n-2}(\tilde{f}_{i,j}) = 0$. By Definition 4.6(3), it suffices to show $b_h(F(\tilde{f}_{i,j})) = b_{h-1}(\tilde{f}_{i,j})$ for $1 \leq h \leq n-1$. By definition, $b_{h-1}(\tilde{f}_{i,j}) = 0$ if and only if $i^+_h + j^+_h < p^h - 1$. By Lemma 2.1(3), this is equivalent to $p - 1 + j_{n-1} + p(i^+_h + j^+_h) < p^{h+1} - 1$. By Proposition 3.6[A], this is equivalent to $b_h(F(\tilde{f}_{i,j})) = 0$. Also notice that $b_0(F(\tilde{f}_{i,j})) = 1$ since $p - 1 + j_{n-1} \geq p - 1$.
   For [B], given $\tilde{f}_{i,j} \in H^1_{\mathrm{dR}}(X_q)_{\vec{b}}$ such that $F(\tilde{f}_{i,j}) \in H^0(X_q, \Omega^1)$, the claim is that $F(\tilde{f}_{i,j}) \in H^1_{\mathrm{dR}}(X_q)_{\vec{F}b}$. By Proposition 3.6, $F(\tilde{f}_{i,j}) \in H^0(X_q, \Omega^1)$ when $b_{n-2}(\tilde{f}_{i,j}) = 1$. By Definition 4.6(4), it suffices to show $b_{k-1}(\tilde{f}_{i,j}) = 0$ if and only if $b_k(F(\tilde{f}_{i,j})) = 1$ for $1 \leq k \leq n-1$. By definition, $b_{k-1}(\tilde{f}_{i,j}) = 0$ if and only if $i^+_k + j^+_k < p^k - 1$. By Lemma 2.1(4), this is equivalent to $2p^{k+1} - 2 - (i^+_k + j^+_k)p - p - j_{n-1} \geq p^{k+1} - 1$. By Proposition 3.6[B], this is equivalent to $b_k(F(\tilde{f}_{i,j})) = 1$. Also note that $b_0(F(\tilde{f}_{i,j})) = 0$ since $p - 2 - j_{n-1} < p - 1$.

Here is a sketch of 3 ways to prove that F or V surjects onto the claimed block. The first method is to compute an explicit pre-image in $H^1_{\mathrm{dR}}(X_q)_{\vec{b}}$ for a given element of $H^1_{\mathrm{dR}}(X_q)_{\vec{F}b}$ or $H^1_{\mathrm{dR}}(X_q)_{\vec{V}b}$. We omit this calculation. The second method is to prove that the blocks $H^1_{\mathrm{dR}}(X_q)_{\vec{b}}$ are irreducible $\mathbb{F}_{q^2}[G]$-modules using [HJ90, 4.7]. The third method is to use Corollary 3.3 to show that F and V either trivialize or act injectively on a block; in the latter case, the action must also be surjective by a dimension count from Lemma 4.3. □

Proof of Theorem 4.5. Suppose $\vec{b} \in (\mathbb{Z}/2)^n$ is such that $T(\vec{b}) = t$.

1. If $T(\vec{b}) \leq 2^{n-1}$, then either $b_{n-1} = 1$ and $b_0 = 0$, or $b_{n-1} = 0$ and $b_0 = 1$. Then $VH^1_{\mathrm{dR}}(X_q)_{\vec{b}} = 0$ by Lemma 3.4 in the former case and by Proposition 3.7 in the latter case.
2. If $T(\vec{b}) > 2^{n-1}$, then either $b_{n-1} = 1$ and $b_0 = 1$, or $b_{n-1} = 0$ and $b_0 = 0$. In

the former case, by Definition 4.6(1) and Proposition 4.7(1),

$$\begin{aligned} T(V\vec{b}) &= 2^{n-1}b_1 + \cdots + 2^2 b_{n-2} + 1 \\ &= 2(2^{n-1} + 2^{n-1}b_1 + \cdots + 2b_{n-2} + 1) - 2^n - 1 = 2t - (2^n + 1). \end{aligned}$$

In the latter case, by Definition 4.6(2) and Proposition 4.7(2),

$$\begin{aligned} T(V\vec{b}) &= 2^{n-1}(1 - b_1) + \cdots + 2^2(1 - b_{n-2}) + 2 + 1 \\ &= 2(2^n - 2^{n-1}b_0 - \ldots - 2b_{n-2}) - 2^n - 1 = 2t - (2^n + 1). \end{aligned}$$

3. If $T(\vec{b})$ is odd, then $b_{n-1} = 1$ and $B_t \subset H^0(X_q, \Omega^1)$. Then $F(B_t) = 0$ by Proposition 4.7(3).
4. Suppose $T(\vec{b})$ is even. If $b_{n-2} = 0$, then Proposition 4.7(4)[A] implies that

$$T(F\vec{b}) = 2^n - (2^n + 2^{n-1} + 2^{n-2}b_0 + \ldots - 2b_{n-3}) = t/2.$$

If $b_{n-2} = 1$, then Propositon 4.7(4)[B] implies that

$$\begin{aligned} T(F\vec{b}) &= 2^{n-2}(1 - b_0) + 2^{n-3}(1 - b_1) + \ldots + 2(1 - b_{n-3}) + 1 \\ &= 2^{n-1} - 2^{n-2}b_0 - \ldots - 2b_{n-3} - b_{n-2} = t/2. \end{aligned}$$

□

5. The Dieudonné modules of the Hermitian curves. In this section, we prove Theorem 5.13 which determines the structure of the p-torsion group scheme $\mathrm{Jac}(X_q)[p]$ for all primes p and $n \in \mathbb{N}$. The result is phrased in terms of the Dieudonné module, which we denote by

$$\mathbb{D}(X_{p^n}) := \mathbb{D}(\mathrm{Jac}(X_{p^n})[p]).$$

Specifically, we prove that the distinct indecomposable factors of $\mathbb{D}(X_{p^n})$ are in bijection with orbits of $\mathbb{Z}/(2^n+1) - \{0\}$ under $\langle \times 2 \rangle$ and compute the multiplicity of each factor. In Section 5.2, we explain how the structure of each indecomposable factor is determined from the combinatorics of the orbit. From this, one can compute the Ekedahl-Oort type of $\mathrm{Jac}(X_q)[p]$ in any specific case but it is hard (and non-illuminating) to find formulae in general.

5.1. Combinatorial properties of orbits. Two elements $s, t \in \mathbb{Z}/(2^n+1) - \{0\}$ are in the same *orbit* under $\langle \times 2 \rangle$ if and only if $2^i s \equiv t \bmod 2^n + 1$ for some $i \in \mathbb{Z}$. Every orbit σ of $\mathbb{Z}/(2^n+1) - \{0\}$ under $\langle \times 2 \rangle$ is *symmetric* in that $(-1)\sigma = \sigma$, because $2^n \equiv -1 \bmod 2^n + 1$.

Definition 5.1. Let $\sigma = (\sigma_1 \ldots, \sigma_r)$ be an orbit of $\mathbb{Z}/(2^n + 1) - \{0\}$ under $\langle \times 2 \rangle$. Let $\sigma_0 = \sigma_r$.

1. The *length* $|\sigma|$ of σ is r.
2. An entry $\sigma_i \in \sigma$ is a *local maximum* if $\sigma_{i-1} < \sigma_i > \sigma_{i+1}$. and is a *local minimum* if $\sigma_{i-1} > \sigma_i < \sigma_{i+1}$. Let $\mathrm{Max}(\sigma)$ (resp. $\mathrm{Min}(\sigma)$) be the set of local maximums (resp. minimums) of σ.
3. The *a-number* of σ is $a(\sigma) = \#\mathrm{Max}(\sigma) = \#\mathrm{Min}(\sigma)$.

Lemma 5.2. *If σ is an orbit of $\mathbb{Z}/(2^n + 1) - \{0\}$ under $\langle \times 2 \rangle$, then $|\sigma|$ is even and $a(\sigma)$ is odd.*

Proof. The length is even since σ is symmetric under -1.

Without loss of generality, suppose $\sigma_1 = \min\{\sigma_i \in \sigma\}$. Since σ is symmetric under -1, the absolute maximum of the entries in σ is $\sigma_{\frac{r}{2}+1}$. More generally, $\sigma_{1+i} \equiv -\sigma_{\frac{r}{2}+i} \bmod \mathbb{Z}/(2^n+1)$. Thus σ can be divided into two parts, termed the left half and the right half.

Consider the number of local minimums and local maximums in σ, excluding σ_1 and $\sigma_{\frac{r}{2}+1}$. On each half, the number of local minimums equals the number of local maximums, by an increasing/decreasing argument. By symmetry, the number of local minimums in the left half equals the number of local maximums in the right half. It follows that the number of local maximums other than $\sigma_{\frac{r}{2}+1}$ is even, so $a(\sigma)$ is odd. □

The next definition measures the distances between the local maximums and minimums of σ.

Definition 5.3.

1. If $\sigma_i \in \mathrm{Min}(\sigma)$, the *left distance* of σ_i is $\ell(\sigma_i) = \min\{j \in \mathbb{N} \mid \sigma_{i-j} \in \mathrm{Max}(\sigma)\}$; and the *right distance* of σ_i is $\rho(\sigma_i) = \min\{j \in \mathbb{N} \mid \sigma_{i+j} \in \mathrm{Max}(\sigma)\}$.
2. If $\sigma_i \in \mathrm{Min}(\sigma)$, the *left parent* of σ_i is $L(\sigma_i)$ where $L(\sigma_i) := \sigma_{i-\ell(\sigma_i)}$; and the *right parent* of σ_i is $R(\sigma_i)$ where $R(\sigma_i) := \sigma_{i+\rho(\sigma_i)}$.

Remark 5.4. The structure of an orbit is determined by the binary expansion of its minimal element, see Proposition 5.11. The symmetric property of the orbits can be used to show that the number of orbits of length $2n$ is the number of binary self-reciprocal polynomials of degree $2n$; which is found in sequence A000048 in the Online Encyclopedia of Integer Sequences [OEI]. The total number of orbits is found in sequence A000016 in [OEI].

5.1.1. Short orbits. Most orbits of $\mathbb{Z}/(2^n+1)-\{0\}$ under $\langle\times 2\rangle$ have maximum length $2n$. The following results about short orbits are used in Proposition 5.11, Corollary 5.16 and Applications 6.1 and 6.4.

Lemma 5.5. *Suppose $n = ck$ for $k \in \mathbb{N}$ odd and let $L = (2^n+1)/(2^c+1)$. The multiplication-by-L group homomorphism $\mathbb{Z}/(2^c+1) \hookrightarrow \mathbb{Z}/(2^n+1)$, given by $\alpha \mapsto L\alpha$, induces a bijection*

$$\beta : \sigma \mapsto \sigma_L$$

between orbits σ of $\mathbb{Z}/(2^c+1)-\{0\}$ under $\langle\times 2\rangle$ and orbits σ_L of $\langle L\rangle \cap (\mathbb{Z}/(2^n+1)-\{0\})$ under $\langle\times 2\rangle$.

Proof. Omitted. □

Lemma 5.6. *Suppose $\hat{\sigma}$ is an orbit of $\mathbb{Z}/(2^n+1)-\{0\}$ under $\langle\times 2\rangle$ with $|\hat{\sigma}| < 2n$. Then $n = ck$ for some $k \in \mathbb{N}$ odd and $\hat{\sigma} = \sigma_L$ for some orbit σ of $\mathbb{Z}/(2^c+1)-\{0\}$ under $\langle\times 2\rangle$.*

Proof. Let $\hat{\sigma}$ be an orbit of length $2c$ where $c < n$. Without loss of generality, suppose $\sigma_1 = \min\{\sigma_i \in \hat{\sigma}\}$. Let $L = \gcd(\sigma_1, 2^{n-1})$ and write $\sigma_1 = LM$. Let M^{-1} be the inverse of M modulo 2^n+1. Then $\sigma_{M^{-1}} = (L, 2L, \ldots, 2^cL, -L, -2L, \ldots, -2^cL)$ is another orbit of $\mathbb{Z}/(2^n+1)-\{0\}$ under $\langle\times 2\rangle$ with length $2c$ and a-number 1. The sequence $L, 2L, \ldots, 2^cL$ is strictly increasing and $2^cL < 2^n+1$. Now, c is the smallest positive integer such that $2^cL \equiv -L \bmod 2^n+1$. Thus $(2^c+1)L = m(2^n+1)$ for some $m \in \mathbb{Z}$. However, the fact that $L < (2^n+1)/2^c$ implies that $(2^c+1)L = 2^n+1$ and so $n = ck$ for some $k \in \mathbb{N}$ odd. Let $\sigma = \frac{1}{L}\hat{\sigma} := (\frac{\sigma_1}{L}, \ldots, \frac{\sigma_r}{L})$. Then σ is an orbit of $\mathbb{Z}/(2^c+1)-\{0\}$ under $\langle\times 2\rangle$ and $\hat{\sigma} = \sigma_L$. □

5.2. The construction of a Dieudonné module for each orbit. We define a Dieudonné module $\mathbb{D}(\sigma)$ for every orbit σ of $\mathbb{Z}/(2^n+1)-\{0\}$ under $\langle\times 2\rangle$ in terms of generators and relations. In the next subsection we prove that these modules are in fact the indecomposable factors of the Dieudonneé module of X_{p^n}.

For convenience, we replace an entry $\sigma_i \in \sigma$ by a variable B_{σ_i}. If $\sigma_i \in \mathrm{Max}(\sigma)$, then B_{σ_i} is a *generator block*. If $\sigma_i \in \mathrm{Min}(\sigma)$, then B_{σ_i} is a *relation block*.

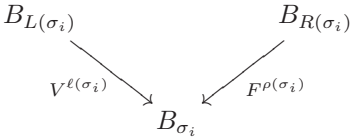
DEFINITION 5.7. Let $\sigma = (\sigma_1 \ldots, \sigma_r)$ be an orbit of $\mathbb{Z}/(2^n+1)-\{0\}$ under $\langle\times 2\rangle$. The Dieudonné module $\mathbb{D}(\sigma)$ is the quotient of the left $\mathbb{E}$-module generated by variables

$$\{B_{\sigma_i} \mid \sigma_i \in \mathrm{Max}(\sigma)\},$$

by the left ideal of relations generated by

$$\{V^{\ell(\sigma_i)}B_{L(\sigma_i)} + F^{\rho(\sigma_i)}B_{R(\sigma_i)} = 0 \mid \text{ for all } \sigma_i \in \mathrm{Min}(\sigma)\}.$$

The following diagram illustrates the definition.

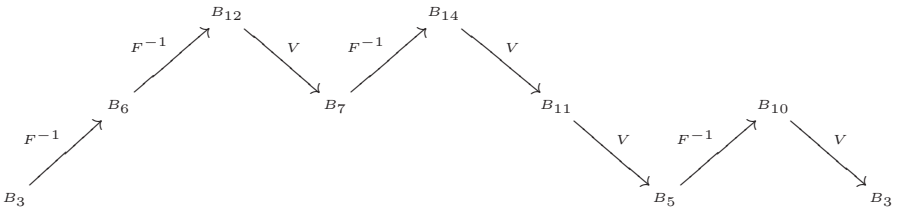


EXAMPLE 5.8. The orbit of 1 in $\mathbb{Z}/(2^n+1)-\{0\}$ under $\langle\times 2\rangle$ is $\sigma = (1, 2, \ldots, 2^n, 2^n-1, \ldots, 2^{n-1}+1)$. It has $a(\sigma) = 1$. The generator block is B_{2^n}. The relation block is B_1. Also $\ell(\sigma_1) = \rho(\sigma_1) = n$. Thus

$$\mathbb{D}(\sigma) \simeq \mathbb{E}/\mathbb{E}(F^n + V^n).$$

This is the Dieudonné module of the unique symmetric BT_1 group scheme of rank p^{2n} having p-rank 0 and a-number 1. This group scheme, which we denote by $I_{n,1}$, has Ekedahl-Oort type $[0, 1, 2, \ldots, n-1]$; see [Pri08, Lemma 3.1] for details.

EXAMPLE 5.9. When $n = 4$, an orbit of $\langle\times 2\rangle$ on $\mathbb{Z}/17$ is $\sigma = \{3, 6, 12, 7, 14, 11, 5, 10\}$ as illustrated below.



It has $a(\sigma) = 3$. The generator blocks are B_{12}, B_{14} and B_{10} and the relation blocks are B_3, B_7, and B_5. The relations are $FB_{14} + VB_{12} = 0$ and $FB_{10} + V^2B_{14} = 0$ and $F^2B_{12} + VB_{10} = 0$. Thus

$$\mathbb{D}(\sigma) = (\mathbb{E}B_{12} \oplus \mathbb{E}B_{14} \oplus \mathbb{E}B_{10})/\mathbb{E}(FB_{14} + VB_{12}, FB_{10} + V^2B_{14}, F^2B_{12} + VB_{10}).$$

Then $\mathbb{D}(\sigma) \simeq \mathbb{D}(I_{4,3})$ where $I_{4,3}$ is the rank 8 BT_1 with Ekedahl-Oort type $[0, 0, 1, 1]$ [EP13, Remark 5.13].

LEMMA 5.10. *The left $\mathbb{E}$-module $\mathbb{D}(\sigma)$ is symmetric, is trivialized by both F and V, has dimension $|\sigma|$, and has a-number $a(\sigma)$.*

Proof. First, $\mathbb{D}(\sigma)$ is symmetric since σ is symmetric. Second, the relations $FV = VF = 0$ imply that $V^{\ell(\sigma_i)+1}B_{L(\sigma_i)} = 0$ and $F^{\rho(\sigma_i)+1}B_{R(\sigma_i)} = 0$ for each $\sigma_i \in \mathrm{Min}(\sigma)$. Since every generator block is both a left and a right parent, powers of F and V trivialize all the generator blocks. Third, the dimension equals the number of distinct images of the generator blocks under powers of F and of V, which is exactly $|\sigma|$. Finally, the a-number equals the number of generators as an $\mathbb{E}$-module. □

PROPOSITION 5.11. *If σ' and σ are distinct orbits of $\mathbb{Z}/(2^n+1) - \{0\}$ under $\langle \times 2 \rangle$, then $\mathbb{D}(\sigma) \not\simeq \mathbb{D}(\sigma')$.*

Proof. By Lemma 5.10(3), the structure of $\mathbb{D}(\sigma)$ determines $|\sigma|$. The bijection β in Lemma 5.5 preserves the $\mathbb{E}$-module structure of the Dieudonné module: $\mathbb{D}(\sigma_L) \simeq \mathbb{D}(\sigma)$. By Lemmas 5.5 and 5.6, it suffices to restrict to the case $|\sigma| = 2n$. Without loss of generality, suppose $\sigma_1 = \min\{\sigma_i \in \sigma\}$. By minimality, $\sigma_1 < 2^{n-1}$ (otherwise $-\sigma_1 < \sigma_1$) and σ_1 is odd. Notice that $\sigma_i > \sigma_{i+1}$ if and only if $\sigma_i > 2^{n-1}$ (the last bit of σ_i equals 1). Since $\sigma_i = 2\sigma_{i-1} \mod 2^n + 1$, the last bit of σ_i is the penultimate bit of σ_{i-1}. By induction, $\sigma_i > \sigma_{i+1}$ if and only if the $(n-i-1)$st bit of σ_1 equals 1 for $1 \le i \le n-1$. Thus the structure of $\mathbb{D}(\sigma)$ determines the binary expansion of σ_1. □

5.3. Main Theorem. For all primes p and $n \in \mathbb{N}$, we find the structure of the Dieudonné module $\mathbb{D}(X_{p^n})$ of the p-torsion group scheme of the Jacobian of the Hermitian curve X_{p^n}. The $\mathbb{E}$-module structure of $\mathbb{D}(X_{p^n})$ is determined by its distinct indecomposable factors, which are in bijection with orbits of $\mathbb{Z}/(2^n+1) - \{0\}$ under $\langle \times 2 \rangle$, and their multiplicities. The $\mathbb{E}$-module structure of each indecomposable factor is determined by the combinatorics of the corresponding orbit, as described in Section 5.2.

DEFINITION 5.12. If $1 \le t \le 2^n$ and $s \equiv 2t \bmod 2^n + 1$, then $\dim_k(B_s) = \dim_k(B_t)$ by Theorem 4.5(2)(4). If σ is an orbit of $\mathbb{Z}/(2^n+1) - \{0\}$ under $\langle \times 2 \rangle$, its *multiplicity* is $m(\sigma) := \dim_k(B_{\sigma_i})$ for any $\sigma_i \in \sigma$.

The multiplicity $m(\sigma)$ was computed in Lemma 4.3.

THEOREM 5.13. *For all primes p and $n \in \mathbb{N}$, there is a bijection between orbits of $\mathbb{Z}/(2^n+1) - \{0\}$ under $\langle \times 2 \rangle$ and distinct indecomposable factors in the Dieudonné module $\mathbb{D}(X_q)$ of $\mathrm{Jac}(X_q)[p]$ given by $\sigma \to \mathbb{D}(\sigma)$. The multiplicity of $\mathbb{D}(\sigma)$ in $\mathbb{D}(X_q)$ is $m(\sigma)$.*

Proof. Suppose σ is an orbit of $\mathbb{Z}/(2^n+1) - \{0\}$ under $\langle \times 2 \rangle$. Consider

$$W_\sigma := \mathrm{Span}_{\sigma_i \in \sigma} B_{\sigma_i} \subset H^1_{\mathrm{dR}}(X_q).$$

By Theorem 4.5, W_σ is stable under the action of V and F^{-1}.

Write $\sigma = (\sigma_1, \ldots, \sigma_r)$, choosing σ_1 to be a local minimum with maximal left distance. Let $B = B_{\sigma_1}$. Define a word $\omega = \omega_r \cdots \omega_1$ in the variables F^{-1} and V as follows: $\omega_i = F^{-1}$ if $1 \le \sigma_i \le 2^{n-1}$ and $\omega_i = V$ if $2^{n-1} + 1 \le \sigma_i \le 2^n$. By Corollary 4.1, the word ω yields an isomorphism $\omega : B \to B$; (it is p^{-r}-linear). Applying Corollary 3.3 shows that ω is represented by a *generalized permutation matrix*, namely a matrix with exactly one non-zero entry in each row and column, with respect to the basis $\mathbb{B} \cap B$. This implies that an iterate of ω can be represented by a diagonal matrix.

In fact, ω itself can be represented by a diagonal matrix; in other words, that there is a basis of eigenvectors for ω. To see this, consider the final filtration for the $\mathbb{E}$-module W_σ as described in Section 2.1.5. First, W_σ has rank p^{rm} where $m = \dim(B)$. It has a canonical filtration $0 = M_0 \subset M_1 \subset \cdots \subset M_r$ where $\dim(M_i) = im$. Here each M_i is a union of blocks B_j from the orbit; in particular, $M_r = W_\sigma$ and $M_1 = B$. The final filtration $N_1 \subset N_2 \subset \cdots \subset N_{rm}$ is a refinement of the canonical filtration, so $N_{im} = M_i$. It is a filtration of W_σ as a k-vector space which is stable under the action of V and F^{-1} such that $i = \dim(N_i)$.

Let x_1 denote a non-zero element of $N_1 \subset M_1 = B$. Since the final filtration is stable under F^{-1} and V, the element $y_1 = \omega_1(x_1) = F^{-1}(x_1)$ generates N_{m+1}/M_1. Similarly, N_{im+1}/M_i is generated by an image of x_1 under a portion of the word ω. Going through the whole word, $\omega(x_1)$ is a generator for N_1/N_0. Thus $\omega(x_1)$ is a constant multiple of x_1.

Thus there is an $\mathbb{E}$-module isomorphism $W_\sigma \simeq \mathbb{D}(\sigma)^{m(\sigma)}$. By Proposition 5.11, the factors $\mathbb{D}(\sigma)$ of $\mathbb{D}(X_q)$ are distinct and are in bijection with orbits $\mathbb{Z}/(2^n+1) - \{0\}$ under $\langle \times 2 \rangle$ □

Recall the definition of *break points* from Section 2.1.5.

COROLLARY 5.14. *The Ekedahl-Oort type ν of X_q has 2^{n-1} break points; in other words, the sequence ν_i alternates between being constant and increasing on 2^{n-1} intervals for $1 \leq i \leq g$. This pattern is consistent for all primes p, although the formulae for the break points depends on p.*

Proof. By Theorem 5.13, the canonical filtration is constructed by successively adjoining the blocks B_t. The behavior of F and V is consistent across each block. Thus there are 2^n canonical fragments, the first half of which determine break points of ν. □

5.4. Indecomposable factors of $\mathbb{D}(X_{p^n})$ with a-number 1. For $c \in \mathbb{N}$, recall from Example 5.8 that $I_{c,1}$ is the unique symmetric BT_1 group scheme of rank p^{2c} having p-rank 0 and a-number 1. In this section, we find the multiplicity of $\mathbb{D}(I_{c,1}) = \mathbb{E}/\mathbb{E}(F^c + V^c)$ in $\mathbb{D}(X_{p^n})$. As motivation, note that $\mathbb{D}(I_{1,1})$ occurs in $\mathbb{D}(X_{p^n})$ exactly when there is a block B_t such that $F(B_t) = V(B_t)$. This can only occur when n is even and $t = (2^{n+1}+2)/3$, in which case the orbit is $\sigma = (t/2, t)$.

We will need the following result about multiplicities of short orbits. If W is an indecomposable factor of $\mathbb{D}(X_{p^c})$ and if $n = ck$ for some odd $k \in \mathbb{N}$, then W is an indecomposable factor of $\mathbb{D}(X_{p^n})$ associated with a short orbit by Lemma 5.5. The next result compares the multiplicity of W in $\mathbb{D}(X_{p^c})$ and $\mathbb{D}(X_{p^n})$.

PROPOSITION 5.15. *Suppose $n = ck$ for $k \in \mathbb{N}$ odd and let $L = (2^n+1)/(2^c+1)$. The multiplicity $M(\sigma)$ of $\mathbb{D}(\sigma)$ in $\mathbb{D}(X_{p^c})$ and the multiplicity $M(\sigma_L)$ of $\mathbb{D}(\sigma_L)$ in $\mathbb{D}(X_{p^n})$ are related by the formula: $M(\sigma_L) = M(\sigma)^k$.*

Proof. Note that $M(\sigma) = \dim_k(B_t)$ where $t = \min\{\sigma_i \in \sigma\}$. Also, $M(\sigma_L) = \dim_k(B_{Lt})$ because $Lt = \min\{\sigma_i \in \sigma_L\}$. Since t is odd, $\vec{b}(t) \in (\mathbb{Z}/2)^a$ is the binary expansion of $t-1$. Note that $L = (2^a-1)(2^{n-2a} + 2^{n-4a} + \cdots + 2^a) + 1$. Now $t(2^a-1) = (t-1)2^a + 2^a - t$ has binary expansion $(\iota(\vec{b}(t)), \vec{b}(t)))$ of length $2a$. Thus $Lt - 1 = t(2^a-1)(2^{n-2a} + 2^{n-4a} + \cdots + 2^a) + (t-1)$ has binary expansion $(\vec{b}(t), \iota(\vec{b}(t)), \vec{b}(t), \ldots, \iota(\vec{b}(t)), \vec{b}(t))$, where the sequence has k terms of length a. As $t < 2^{n-1}$ the result follows from Lemma 4.3. □

Recall from Proposition 3.5 that the rank of $\mathcal{C}^i$ on $H^0(X_q, \Omega^1)$ is $r_{n,i} = p^n(p+1)^i(p^{n-i}-1)/2^{i+1}$.

COROLLARY 5.16.

1. *The Dieudonné module* $\mathbb{D}(I_{n,1})$ *occurs with multiplicity* $r_{n,n-1}$ *in* $\mathbb{D}(X_{p^n})$.
2. *The Dieudonné module* $\mathbb{D}(I_{c,1})$ *appears as an indecomposable factor of* $\mathbb{D}(X_{p^n})$ *if and only if* $n = ck$ *for some odd* $k \in \mathbb{N}$, *in which case the multiplicity of* $\mathbb{D}(I_{c,1})$ *in* $\mathbb{D}(X_{p^n})$ *is* $M(I_{c,1}) := (r_{c,c-1})^k$.
3. *If* $n \in \mathbb{N}$ *is even, then the multiplicity of* $\mathbb{D}(I_{1,1})$ *in* $\mathbb{D}(X_{p^n})$ *is zero. If* $n \in \mathbb{N}$ *is odd, then the multiplicity of* $\mathbb{D}(I_{1,1})$ *in* $\mathbb{D}(X_{p^n})$ *is* $(p(p-1)/2)^n$.

REMARK 5.17. Corollary 5.16 is equivalent to the fact that $\mathrm{Ker}(F^n) = \mathrm{Ker}(V^n)$ has dimension $2g - r_{n,n-1}$ in $H^1_{dR}(X_{p^n})$ or the fact that $\mathrm{Im}(F^n) = \mathrm{Im}(V^n)$ has dimension $r_{n,n-1}$ in $H^1_{dR}(X_{p^n})$.

Proof.

1. By Example 5.8, $\mathbb{D}(I_{n,1}) = \mathbb{D}(\sigma)$ for the orbit σ containing 1. Then $M(\sigma)$ equals the dimension of $B_1 = V^n B_{2^n}$, which equals the rank $r_{n,n-1}$ of $\mathcal{C}$ on $H^0(X_q, \Omega^1)$.
2. By part 1, one can suppose that $1 \leq c < n$. Then $\mathrm{rank}(\mathbb{D}(I_{c,1})) < p^{2n}$. Thus, if $\mathbb{D}(I_{c,1})$ occurs in $\mathbb{D}(X_{p^n})$, then $\mathbb{D}(I_{c,1}) = \mathbb{D}(\hat{\sigma})$ for a short orbit $\hat{\sigma}$ of $\mathbb{Z}/(2^n+1) - \{0\}$. By Lemma 5.6, $n = ck$ for some $k \in \mathbb{N}$ odd. Suppose $n = ck$ for some $k \in \mathbb{N}$ odd. By part 1, $\mathbb{D}(I_{c,1})$ appears in $\mathbb{D}(X_{p^c})$ with multiplicity $r_{c,c-1}$. The result then follows from Lemma 5.5 and Proposition 5.15.
3. This follows from part 2, setting $c = 1$.

□

As an example, consider the case $n = 4$, which involves the rank 8 group scheme $I_{4,3}$ from Example 5.9.

EXAMPLE 5.18. The Dieudonné module $\mathbb{D}(X_{p^4})$ of $\mathrm{Jac}(X_{p^4})[p]$ is:

$$\mathbb{D}(X_{p^4}) = (\mathbb{E}/\mathbb{E}(F^4 + V^4))^{r_{4,3}} \oplus (\mathbb{D}(I_{4,3}))^{r_{4,1} - 3r_{4,3}}. \tag{5}$$

Proof. The orbit $\sigma = \{1, 2, 4, 8, 16, 15, 13, 9\}$ has $\mathbb{D}(\sigma) = \mathbb{D}(I_{4,1})$. The multiplicity of $\mathbb{D}(I_{4,1})$ is determined by Corollary 5.16(1). There is one other orbit $\sigma' = \{3, 6, 12, 7, 14, 11, 5, 10\}$ of $\langle \times 2 \rangle$ on $\mathbb{Z}/17$. By Example 5.9, $\mathbb{D}(\sigma') = \mathbb{D}(I_{4,3})$. The multiplicity of $\mathbb{D}(I_{4,3})$ equals $(2g - 8r_{4,3})/8$. □

6. Applications.

6.1. Decomposition of Jacobians of Hermitian curves. The fact that $\mathrm{Jac}(X_{p^n})$ is supersingular is equivalent to the fact that it decomposes, up to isogeny, into a product of supersingular elliptic curves:

$$\mathrm{Jac}(X_{p^n}) \sim \times_{i=1}^{g} E_i.$$

A more refined problem is about the decomposition of $\mathrm{Jac}(X_{p^n})$ up to isomorphism. Consider an isomorphism

$$\mathrm{Jac}(X_{p^n}) \simeq \times_{i=1}^{N} A_i$$

of abelian varieties without polarization, where each A_i is indecomposable and $g = \sum_{i=1}^{N} \dim(A_i)$.

When $n = 1$, Section 2.2.1 and [Oor75, Theorem 2] imply that the Jacobian of X_p is isomorphic to a product of supersingular elliptic curves:

$$\mathrm{Jac}(X_p) \simeq \times_{i=1}^{g} E_i.$$

For $n \geq 2$, we did not find any results about the decomposition of $\mathrm{Jac}(X_{p^n})$ up to isomorphism in the literature. In this section, we use Theorem 5.13 to provide constraints on this decomposition.

6.1.1. Elliptic rank. If A is an abelian variety, its *elliptic rank* is the largest non-negative integer r such that there exist elliptic curves $E_1, \ldots, E_r$ and an abelian variety B of dimension $g-r$ and an isomorphism $A \simeq B \times (\times_{i=1}^{r} E_i)$ of abelian varieties without polarization.

Application 6.1. *If n is even, then the elliptic rank of* $\mathrm{Jac}(X_{p^n})$ *is* 0. *If n is odd, then the elliptic rank of* $\mathrm{Jac}(X_{p^n})$ *is at most* $(p(p-1)/2)^n$.

Proof. If $\mathrm{Jac}(X_{p^n}) \simeq B \times (\times_{i=1}^{r} E_i)$, then each E_i is supersingular and $\mathbb{D}(E_i) \simeq \mathbb{E}/\mathbb{E}(F+V)$. The result follows from Corollary 5.16(3) since the elliptic rank is bounded by the multiplicity of $\mathbb{D}(I_{1,1})$ in $\mathbb{D}(X_{p^n})$. □

6.1.2. A partition condition on the decomposition. We determine a partition condition on the decomposition of the Jacobian $\mathrm{Jac}(X_{p^n})$ up to isomorphism, starting with a simple-to-state application.

Application 6.2. *Suppose $n = 2^e$ for some $e \in \mathbb{N}$ and suppose* $\mathrm{Jac}(X_{p^n}) \simeq \times_{i=1}^{N} A_i$. *Then $n \mid \dim(A_i)$ for $1 \leq i \leq N$ and $N \leq g/n$. In particular, when $n = 2$, then* $\dim(A_i)$ *is even for all $1 \leq i \leq N$.*

Proof. If $n = 2^e$, then all orbits σ of $\mathbb{Z}/(2^n+1) - \{0\}$ have length exactly $2n$. By Lemma 5.10, $\dim(\mathbb{D}(\sigma)) = 2n$. Also $\mathbb{D}(A_i)$ has dimension $2\dim(A_i)$ and is a direct sum of Dieudonné modules of dimension $2n$. □

Definition 6.3. Consider two partitions η_J and $\eta_{\mathbb{D}}$ defined as follows. If $J \simeq \times_{i=1}^{N} A_i$, where each A_i is an indecomposable abelian variety, let $\eta_J = \{\dim(A_i) \mid 1 \leq i \leq N\}$. If $\mathbb{D}(X_{p^n}) = \oplus_{i=1}^{\delta} D_i$, where each D_i is an indecomposable symmetric Dieudonné module, let $\eta_{\mathbb{D}} = \{\dim(D_i) \mid 1 \leq i \leq \delta\}$.

It is clear that the partition $\eta_{\mathbb{D}}$ is a refinement of the partition η_J. For any q, this observation can be used to compute a lower bound for the partition η_J which is the set of dimensions of the indecomposable factors in the decomposition of $\mathrm{Jac}(X_{p^n})$ up to isomorphism. In particular, this yields the upper bound $N \leq \sum_\sigma m(\sigma)$. For example, when $n = 3$, then $N \leq g - 2r_{3,2} \sim g/2$.

6.2. Application to Selmer groups. Let A be an abelian variety defined over the function field K of X_q with $q = p^n$. Let $f : A \to A'$ be an isogeny of abelian varieties over K. Recall that the Tate-Shafarevich group $Ш(K, A)$ is the kernel of $H^1(K, A) \to \prod_v H^1(K_v, A)$ where the product is taken over all places v of K. Let $Ш(K, A)_f$ be the kernel of the induced map $Ш(K, A) \to Ш(K, A')$. Also define the local Selmer group $\mathrm{Sel}(K_v, f)$ to be the image of the coboundary map $A'(K_v) \to H^1(K_v, \mathrm{Ker}(f))$ and the global Selmer group to be the subset of $H^1(K, \mathrm{Ker}(f))$ which restrict to elements of $\mathrm{Sel}(K_v, f)$ for all v. There is an exact sequence

$$0 \to A'(K)/f(A(K)) \to \mathrm{Sel}(K, f) \to Ш(K, A)_f \to 0.$$

In [Dum99, Theorems 1 & 2], the author determines the group structure of $Ш$ in the case when A is $\mathrm{Jac}(X_q)$ or A is a supersingular elliptic factor of $\mathrm{Jac}(X_q)$. Here is a quick application about this topic.

APPLICATION 6.4. *Let E be a constant elliptic curve over the function field K of X_q. If E is ordinary, then* $\mathrm{Sel}(K,[p])$ *has rank* $2r_{n,1} = p^n(p+1)(p^{n-1}-1)/2$.

Proof. The result follows from Proposition 3.5 because the rank of $\mathrm{Sel}(K,[p])$ is twice the rank of $\mathcal{C}$ [Ulm91, Proposition 3.3]. □

6.3. Application about the supersingular locus. The moduli space $\mathcal{A}_g$ of principally polarized abelian varieties of dimension g can be stratified by Ekedahl-Oort type into locally closed strata. By [Oor13, Lemma 10.13], the stratum for the Ekedahl-Oort type ν is contained in the supersingular locus S_g if and only if $\nu_s = 0$ where $s = \lceil g/2 \rceil$.

Each generic point of S_g has a-number 1 [LO98, Section 4.9]. By Example 5.8, the unique Ekedahl-Oort type with p-rank 0 and a-number 1 has $\nu_s = s-1$ which is not zero for $g \geq 3$. Thus this Ekedahl-Oort stratum intersects but is not contained in S_g.

For all p, we give infinitely many new examples of Ekedahl-Oort strata which intersect but are not contained in S_g. What is significant is that each has large a-number, namely just a bit smaller than $g/2$. Note that $a \leq \lfloor (g-1)/2 \rfloor$ is the smallest upper bound for a which guarantees that $\nu_s \neq 0$.

APPLICATION 6.5. *Let $q = p^n$ with $n \geq 3$ and let $g = q(q-1)/2$. The Hermitian curve X_q has a-number $\frac{g}{2}[1 - \frac{p}{q}\frac{p^{n-2}-1}{q-1}]$. Its Ekedahl-Oort stratum intersects, but is not contained in, the supersingular locus of $\mathcal{A}_g$.*

Proof. The Jacobian of the Hermitian curve X_{p^n} is supersingular and has dimension g. Let ν be its Ekedahl-Oort type and let η be the strata of $\mathcal{A}_g$ with Ekedahl-Oort type ν. By Proposition 3.5, $\nu_i = 0$ if and only if $i \leq r_{n,n-1} = p^n(p+1)^{n-1}(p-1)/2^n$. By [Oor13, Lemma 10.13], $\eta \subset S_g$ if and only if $\nu_s = 0$ where $s = \lceil g/2 \rceil$. This condition is not satisfied for $n \geq 3$. □

REFERENCES

[Car57] P. CARTIER, *Une nouvelle opération sur les formes différentielles*, C. R. Acad. Sci. Paris, 244 (1957), pp. 426–428.

[Dem86] M. DEMAZURE, *Lectures on p-divisible groups*, Lecture Notes in Mathematics, vol. 302, Springer-Verlag, Berlin, 1986, Reprint of the 1972 original.

[Dum95] N. DUMMIGAN, *The determinants of certain Mordell-Weil lattices*, Amer. J. Math., 117:6 (1995), pp. 1409–1429.

[Dum99] ———, *Complete p-descent for Jacobians of Hermitian curves*, Compositio Math., 119:2 (1999), pp. 111–132.

[Eke87] T. EKEDAHL, *On supersingular curves and abelian varieties*, Math. Scand., 60:2 (1987), pp. 151–178.

[EP13] A. ELKIN AND R. PRIES, *Ekedahl-Oort strata of hyperelliptic curves in characteristic 2*, Algebra Number Theory, 7:3 (2013), pp. 507–532.

[EvdG09] T. EKEDAHL AND G. VAN DER GEER, *Cycle classes of the E-O stratification on the moduli of abelian varieties*, Algebra, arithmetic, and geometry: in honor of Yu. I. Manin. Vol. I, Progr. Math., vol. 269, Birkhäuser Boston Inc., Boston, MA, 2009, pp. 567–636.

[Gor02] E. GOREN, *Lectures on Hilbert modular varieties and modular forms*, CRM Monograph Series, vol. 14, American Mathematical Society, Providence, RI, 2002, With M.-H. Nicole.

[Gro90] B. H. GROSS, *Group representations and lattices*, J. Amer. Math. Soc., 3:4 (1990), pp. 929–960.

[GSX00] A. GARCIA, H. STICHTENOTH, AND C.-P. XING, *On subfields of the Hermitian function field*, Compositio Math., 120:2 (2000), pp. 137–170.

[Han92] J. P. Hansen, *Deligne-Lusztig varieties and group codes*, Coding theory and algebraic geometry (Luminy, 1991), Lecture Notes in Math., vol. 1518, Springer, Berlin, 1992, pp. 63–81.

[HJ90] B. Haastert and J. C. Jantzen, *Filtrations of the discrete series of* $\mathrm{SL}_2(q)$ *via crystalline cohomology*, J. Algebra, 132:1 (1990), pp. 77–103.

[Kra] H. Kraft, *Kommutative algebraische p-Gruppen (mit Anwendungen auf p-divisible Gruppen und abelsche Varietäten)*, Sonderforsch. Bereich Bonn, September 1975, 86 pp.

[Lau99] K. Lauter, *Deligne-Lusztig curves as ray class fields*, Manuscripta Math., 98:1 (1999), pp. 87–96.

[LO98] K.-Z. Li and F. Oort, *Moduli of supersingular abelian varieties*, Lecture Notes in Mathematics, vol. 1680, Springer-Verlag, Berlin, 1998.

[Moo01] B. Moonen, *Group schemes with additional structures and Weyl group cosets*, Moduli of abelian varieties (Texel Island, 1999), Progr. Math., vol. 195, Birkhäuser, Basel, 2001, pp. 255–298.

[Nyg81] N. O. Nygaard, *Slopes of powers of Frobenius on crystalline cohomology*, Ann. Sci. École Norm. Sup. (4), 14:4 (1981), pp. 369–401 (1982).

[Oda69] T. Oda, *The first de Rham cohomology group and Dieudonné modules*, Ann. Sci. École Norm. Sup. (4), 2 (1969), pp. 63–135.

[OEI] *The On-Line Encyclopedia of Integer Sequences*, `http://oeis.org`.

[Oor74] F. Oort, *Subvarieties of moduli spaces*, Invent. Math., 24 (1974), pp. 95–119.

[Oor75] ———, *Which abelian surfaces are products of elliptic curves?*, Math. Ann., 214 (1975), pp. 35–47.

[Oor01] ———, *A stratification of a moduli space of abelian varieties*, Moduli of abelian varieties (Texel Island, 1999), Progr. Math., vol. 195, Birkhäuser, Basel, 2001, pp. 345–416.

[Oor13] ———, *Moduli of abelian varieties in mixed and in positive characteristic*, Handbook of moduli (Eds Gavril Farkas & Ian Morrison), Vol. III, pp. 75–134. Advanced Lectures in Mathematics, 25, International Press, 2013.

[Pri08] ———, *A short guide to p-torsion of abelian varieties in characteristic p*, Computational arithmetic geometry, Contemp. Math., vol. 463, Amer. Math. Soc., Providence, RI, 2008, pp. 121–129.

[Pri09] ———, *The p-torsion of curves with large p-rank*, Int. J. Number Theory, 5:6 (2009), pp. 1103–1116.

[RS94] H.-G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math., 457 (1994), pp. 185–188.

[Sti73] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe*, Arch. Math. (Basel), 24 (1973), pp. 527–544.

[Sti09] ———, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009.

[Sul75] F. J. Sullivan, *p-torsion in the class group of curves with too many automorphisms*, Arch. Math. (Basel), 26 (1975), pp. 253–261.

[Ulm91] D. L. Ulmer, *p-descent in characteristic p*, Duke Math. J., 62:2 (1991), pp. 237–265.