manuscripta mathematica manuscript No.
(will be inserted by the editor)

Darren Glass[1] · Rachel Pries[2]

Hyperelliptic curves with prescribed p-torsion

Abstract. In this paper, we show that there exist families of curves (defined over an algebraically closed field k of characteristic $p > 2$) whose Jacobians have interesting p-torsion. For example, for every $0 \leq f \leq g$, we find the dimension of the locus of hyperelliptic curves of genus g with p-rank at most f. We also produce families of curves so that the p-torsion of the Jacobian of each fibre contains multiple copies of the group scheme α_p. The method is to study curves which admit an action by $(\mathbb{Z}/2)^n$ so that the quotient is a projective line. As a result, some of these families intersect the hyperelliptic locus $\mathcal{H}_g$.

1. Introduction

When investigating abelian varieties defined over an algebraically closed field k of characteristic p, it is natural to study the invariants related to their p-torsion such as their p-rank or a-number. Such invariants are well-understood and have been used to define stratifications of the moduli space $\mathcal{A}_g$ of principally polarized abelian varieties of dimension g. There is a deep interest in understanding whether the Torelli locus intersects such strata in $\mathcal{A}_g$. More generally, one can ask for the dimension of the intersection of these strata with the image of the moduli spaces $\mathcal{M}_g$ or $\mathcal{H}_g$ under the Torelli map. In this paper, we show that the Torelli locus intersects several of these strata by producing families of curves so that the p-torsion of the Jacobian of each fibre contains certain group schemes.

Recall that the group scheme $\mu_p = \mu_{p,k}$ is the kernel of Frobenius on $\mathbb{G}_m$ and the group scheme $\alpha_p = \alpha_{p,k}$ is the kernel of Frobenius on $\mathbb{G}_a$. As schemes, $\mu_p \simeq \mathrm{Spec}(k[x]/(x-1)^p)$ and $\alpha_p \simeq \mathrm{Spec}(k[x]/x^p)$ over k. If $\mathrm{Jac}(X)$ is the Jacobian of a k-curve X, the *p-rank* of X is $\dim_{\mathbb{F}_p} \mathrm{Hom}(\mu_p, \mathrm{Jac}(X))$ and the *a-number* of X is $\dim_k \mathrm{Hom}(\alpha_p, \mathrm{Jac}(X))$.

Let $V_{g,f}$ denote the sublocus of $\overline{\mathcal{M}}_g$ consisting of curves of genus g with p-rank at most f. For every g and every $0 \leq f \leq g$, the locus $V_{g,f}$ has codimension $g-f$ in $\overline{\mathcal{M}}_g$, [1]. In Section 2, we use results from [1] to prove that there exist smooth hyperelliptic curves of genus g with every possible p-rank f.

The authors were partially supported by NSF VIGRE grant DMS-98-10750.

D. Glass: Department of Mathematics, Columbia University, New York, NY 10027 e-mail: glass@math.columbia.edu

R. Pries: 101 Weber Building, Colorado State University, Fort Collins, CO 80523-1874 e-mail: pries@math.colostate.edu

Theorem 1. For all $g \geq 1$ and all $0 \leq f \leq g$, the locus $V_{g,f} \cap \mathcal{H}_g$ is non-empty of dimension $g-1+f$. In particular, there exists a smooth hyperelliptic curve of genus g and p-rank f.

Let $T_{g,a}$ denote the sublocus of $\overline{\mathcal{M}}_g$ consisting of curves of genus g with a-number at least a. In Section 5, we show that $T_{g,a}$ is non-empty under certain conditions on g and a by producing curves X so that $\mathrm{Jac}(X)[p]$ contains multiple copies of α_p. Let $\mathcal{H}_{g,n}$ be the sublocus of the moduli space $\mathcal{M}_g$ consisting of smooth curves of genus g which admit an action by $(\mathbb{Z}/2)^n$ so that the quotient is a projective line.

Corollary 3. Suppose $n \geq 2$ and $p \geq 2n+1$. Suppose g is such that $\mathcal{H}_{g,n}$ is non-empty of dimension at least $n+1$. Then the intersection $\mathcal{H}_{g,n} \cap T_{g,n}$ has codimension at most n in $\mathcal{H}_{g,n}$. In particular, there exists a smooth curve of genus g with a-number at least n.

The dimension of the family in Corollary 3 is at least $(g+2^n-1)/2^{n-2}-3-n$. The precise numerical conditions for g can be found in Section 5. The main interest in this result is not only that certain group schemes occur in the p-torsion of the Jacobians, but also that the dimension of the families is large in comparison with the dimension of $\mathcal{H}_{g,n}$.

For small values of n, we further show that these families of curves intersect the hyperelliptic locus $\mathcal{H}_g$, resulting in the following corollaries.

Corollary 4. Suppose $g \geq 2$ and $p \geq 5$. There exists a $(g-2)$-dimensional family of smooth hyperelliptic curves of genus g whose fibres have a-number 2 and p-rank $g-2$.

Corollary 5. Suppose $g \geq 5$ is odd and $p \geq 7$. There exists a $(g-5)/2$-dimensional family of smooth hyperelliptic curves of genus g whose fibres have a-number at least 3.

In Section 6, we consider the problem of constructing Jacobians whose p-torsion contains group schemes other than μ_p or α_p. We prove that for all $g \geq 2$ there exists a smooth hyperelliptic curve of genus g whose p-torsion contains the group scheme corresponding to a supersingular non-superspecial abelian surface. We describe this group scheme and its covariant Dieudonné module in Section 6. It has a-number 1 and p-rank 0.

Our method for these results is to analyze the curves in the locus $\mathcal{H}_{g,n}$ in terms of fibre products of hyperelliptic curves. In Section 3, we extend results of Kani and Rosen [8] to compare the p-torsion of the Jacobian of a curve X in $\mathcal{H}_{g,n}$ to the p-torsion of the Jacobians of its $\mathbb{Z}/2\mathbb{Z}$-quotients *up to isomorphism*. We then use Yui's description of the branch locus of a non-ordinary hyperelliptic curve, [17]. In some cases, this reduces the study of the p-torsion of the Jacobian of X to the study of the intersection of some subvarieties in the configuration space of branch points. We consider this in Section 4.

Throughout, k is an algebraically closed field of characteristic $p > 2$. We assume $g \geq 1$ to avoid trivial cases. Without further comment, we will speak of a *fibre* of a relative curve when we mean a geometric fibre.

This paper led us to pose some open questions on this topic in [2].

2. Curves with prescribed p-rank

We begin by considering the p-rank of Jacobians of hyperelliptic curves. Recall that the p-rank, $\dim_{\mathbb{F}_p} \mathrm{Hom}(\mu_p, \mathrm{Jac}(X))$, of a k-curve X is an integer between 0 and its genus g. The curve X is said to be *ordinary* if it has p-rank equal to g. In other words, X is ordinary if $\mathrm{Jac}(X)[p] \cong (\mathbb{Z}/p \oplus \mu_p)^g$. Let $V_{g,f}$ denote the sublocus of $\overline{\mathcal{M}}_g$ consisting of curves of genus g with p-rank at most f.

Consider the moduli space $\mathcal{H}_g$ of smooth hyperelliptic curves of genus g and its closure $\overline{\mathcal{H}}_g$ in $\overline{\mathcal{M}}_g$. It is known that $\mathcal{H}_g$ is affine of dimension $2g-1$. Both $\mathcal{H}_g$ and $\overline{\mathcal{H}}_g$ are smooth algebraic stacks over $\mathbb{Z}[1/2]$ (for example, see [16, Proposition 1]). Since k is an algebraically closed field, this fact implies that if two subvarieties of $\overline{\mathcal{H}}_g$ intersect then the codimension of their intersection is at most the sum of their codimensions.

The boundary $\overline{\mathcal{H}}_g - \mathcal{H}_g$ consists of components Δ_0 and Δ_i for integers $1 \leq i \leq g/2$. The generic point of Δ_i corresponds to the isomorphism class of a singular curve with two irreducible components X_i and X_{g-i} intersecting in a node which we denote P_i. Here X_i (resp. X_{g-i}) is a hyperelliptic curve of genus i (resp. $g-i$) and the point P_i is fixed by the hyperelliptic involution on X_i (resp. X_{g-i}). The generic point of Δ_0 corresponds to the isomorphism class of an irreducible hyperelliptic curve X_0' with a node. The normalization X_0 of X_0' is a hyperelliptic curve of genus $g-1$, and the inverse image of the node in X_0' consists of two distinct points in X_0 which are exchanged by the hyperelliptic involution. Note that $\mathrm{Jac}(X_0')$ is a semi-abelian variety and the toric part of its p-torsion contains a copy of the group scheme μ_p. So $\Delta_0 \cap V_{g,0}$ is empty in $\overline{\mathcal{M}}_g$.

We first show that each component of $V_{g,0} \cap \overline{\mathcal{H}}_g$ has dimension $g-1$.

Proposition 1. *The locus $V_{g,0} \cap \overline{\mathcal{H}}_g$ is pure of codimension g in $\overline{\mathcal{H}}_g$.*

Proof. We work by induction on g. The statement is true in the case $g = 1$ since the locus of supersingular elliptic curves has dimension 0. Assume that the statement is true for all $g' < g$, and consider any component C_0 of the intersection $V_{g,0} \cap \overline{\mathcal{H}}_g$. By the purity argument of [10, 1.6], the codimension of C_0 in $\overline{\mathcal{H}}_g$ is at most g. Furthermore, C_0 intersects the boundary of $\overline{\mathcal{H}}_g$ because $\mathcal{H}_g$ is affine. Since C_0 does not intersect Δ_0, it must intersect Δ_i for some $1 \leq i \leq g/2$. We fix one such Δ_i and consider the dimension of the intersection.

A curve corresponding to a point in the intersection of C_0 and Δ_i is formed from two hyperelliptic curves X_i and X_{g-i} which must both have p-rank 0. Thus X_i corresponds to a point of $V_{i,0} \cap \overline{\mathcal{H}}_i$ and likewise X_{g-i} corresponds to a point of $V_{g-i,0} \cap \overline{\mathcal{H}}_{g-i}$. By the inductive hypothesis, there is at most an $i-1$ (resp. $g-i-1$)

dimensional family of choices for X_i (resp. X_{g-i}). Since X_i and X_{g-i} intersect in a unique point P_i, this point must be fixed under the hyperelliptic involutions of the two curves. Thus there are only finitely many choices for the point P_i. It follows that $\dim(C_0 \cap \Delta_i) \leq (i-1)+(g-i-1)+0 = g-2$ and the codimension of $C_0 \cap \Delta_i$ in $\overline{\mathcal{H}}_g$ is at least $g+1$.

We can deduce that $\mathrm{codim}(C_0 \cap \Delta_i) \leq \mathrm{codim}(C_0)+1$ in $\overline{\mathcal{H}}_g$ from the fact that Δ_i has codimension 1 in $\overline{\mathcal{H}}_g$. This implies that the codimension of C_0 in $\overline{\mathcal{H}}_g$ is exactly g and therefore that $V_{g,0} \cap \overline{\mathcal{H}}_g$ is pure of codimension g in $\overline{\mathcal{H}}_g$.

Next we show that each component of $V_{g,f} \cap \overline{\mathcal{H}}_g$ has dimension $g-1+f$ (for $g \geq 1$).

Proposition 2. *The locus $V_{g,f} \cap \overline{\mathcal{H}}_g$ is pure of codimension $g-f$ in $\overline{\mathcal{H}}_g$.*

Proof. By Proposition 1, we can suppose $f \geq 1$. Consider a component C_0 of $V_{g,f} \cap \overline{\mathcal{H}}_g$. By [10, 1.6], C_0 has codimension at most $g-f$ in $\overline{\mathcal{H}}_g$ and thus dimension at least $g-1+f$. Because $p>2$, a complete subvariety of $\overline{\mathcal{H}}_g - \Delta_0$ has dimension at most $g-1$, by [1, Lemma 2.6]. So C_0 intersects Δ_0.

A point of $C_0 \cap \Delta_0$ corresponds to a curve X_0' self-intersecting in a node P_0. The normalization X_0 of X_0' is a hyperelliptic curve of genus $g-1$. Since the toric part of $\mathrm{Jac}(X_0')[p]$ contains a copy of the group scheme μ_p, this implies that the p-rank of X_0 is at most $f-1$. So X_0 corresponds to a point of $V_{g-1,f-1} \cap \overline{\mathcal{H}}_g$. The choice of the nodal point P_0 is equivalent to a choice of two distinct points of X_0 which are exchanged by the hyperelliptic involution. So $\dim(C_0 \cap \Delta_0) = \dim(V_{g-1,f-1} \cap \overline{\mathcal{H}}_g)+1$.

Furthermore, $\mathrm{codim}(C_0) \geq \mathrm{codim}(C_0 \cap \Delta_0) - \mathrm{codim}(\Delta_0)$ in $\overline{\mathcal{H}}_g$. A calculation shows that the codimension of C_0 in $\overline{\mathcal{H}}_g$ is at least the codimension of $V_{g-1,f-1} \cap \overline{\mathcal{H}}_{g-1}$ in $\overline{\mathcal{H}}_{g-1}$. Repeating this calculation, we see that the codimension of C_0 in $\overline{\mathcal{H}}_g$ is at least the codimension of $V_{g-f,0} \cap \overline{\mathcal{H}}_{g-f}$ in $\overline{\mathcal{H}}_{g-f}$, which by Proposition 1 is $g-f$. It follows that $V_{g,f} \cap \overline{\mathcal{H}}_g$ is pure of codimension $g-f$ in $\overline{\mathcal{H}}_g$.

This is the main result in the paper on the p-rank of hyperelliptic curves.

Theorem 1. *For all $g \geq 1$ and all $0 \leq f \leq g$, the locus $V_{g,f} \cap \mathcal{H}_g$ is non-empty of dimension $g-1+f$. In particular, there exists a smooth hyperelliptic curve of genus g and p-rank f.*

Proof. By [1, Proposition 2.7], there exists a smooth hyperelliptic curve X of genus g and p-rank equal to zero for all $g \geq 1$. For $0 \leq f \leq g$, let C_f be the component of $V_{g,f} \cap \overline{\mathcal{H}}_g$ containing X. By Proposition 2, C_f has codimension $g-f$ in $\overline{\mathcal{H}}_g$. It follows that $C_f \cap \mathcal{H}_g$ has dimension $g-1+f$ since C_f is not contained in the boundary of $\overline{\mathcal{H}_g}$. Now C_{f-1} has codimension only $g-f+1$ in $\overline{\mathcal{H}}_g$. So the generic point of C_f is a smooth hyperelliptic curve with p-rank exactly f.

We now turn to the question of constructing Jacobians of curves with large a-number. To do this, we first analyze the Jacobians of fibre products of hyperelliptic curves in Section 3 and then analyze the geometry of the branch points of non-ordinary hyperelliptic curves in Section 4. Unless specified otherwise, the results in the next two sections are also valid in characteristic 0 (but not in characteristic 2).

3. Fibre products of hyperelliptic curves

Let G be an elementary abelian 2-group of order 2^n. In this section, we describe G-Galois covers $\phi : X \to \mathbb{P}^1_k$ where X is a smooth projective k-curve of genus g. For such a cover ϕ, we show that the Jacobian of X decomposes into $2^n - 1$ factors which are Jacobians as well. We study some geometric properties of the Hurwitz space $H_{g,n}$ which parametrizes isomorphism classes of such covers ϕ.

3.1. The moduli space $H_{g,n}$

We first recall a result about the coarse moduli space parametrizing isomorphism classes of G-Galois covers $\phi : X \to \mathbb{P}^1_k$ where X is a smooth projective k-curve of genus g. This description is related to the theory of Hurwitz schemes and gives a framework to describe these covers. In particular, this framework allows one to consider families of such covers with varying branch locus, to lift such a cover from characteristic p to characteristic 0, or to study the locus in $\mathcal{M}_g$ of curves with a certain type of action by G.

To be precise, let $F_{g,n}$ be the contravariant functor which associates to any k-scheme Ω the set of isomorphism classes of $(\mathbb{Z}/2)^n$-Galois covers $\phi_\Omega : X_\Omega \to \mathbb{P}^1_\Omega$ where X is a flat Ω-curve whose fibres are smooth projective curves of genus g and where the branch locus B of ϕ_Ω is a simple horizontal divisor. In other words, the branch locus consists of Ω-points of $\mathbb{P}^1_\Omega$ which do not intersect. Since each inertia group is a cyclic group of order 2, the Riemann-Hurwitz formula implies $g = 2^{n-2}|B| - 2^n + 1$. The following facts about the Hurwitz scheme which coarsely represents this functor are well-known over the complex numbers.

Lemma 1. *i) There exists a coarse moduli space $H_{g,n}$ for the functor $F_{g,n}$ which is of finite type over $\mathbb{Z}[1/2]$.*
ii) There is a natural morphism $\tau : H_{g,n} \to \mathcal{M}_g$ whose fibres have dimension three.
iii) There is a natural morphism $\beta : H_{g,n} \to \mathbb{P}^{|B|}$ which is proper and étale over the image.

Proof. See [15, Chapter 10] for the construction of $H_{g,n}$ and the morphisms τ and β over $\mathbb{C}$. The corresponding statements over $\mathbb{Z}[1/2]$ follow from [16, Theorem 4].

We recall some of the details about the morphisms τ and β. The morphism τ associates to any Ω-point of $H_{g,n}$ the isomorphism class of X_Ω, where $\phi_\Omega : X_\Omega \to \mathbb{P}^1_\Omega$ is the corresponding cover of Ω-curves. The fibres have dimension three since X_Ω is isotrivial if and only if after an étale base change from Ω to Ω' there is a projective linear transformation ρ such that $\rho\phi_{\Omega'}$ is constant, [12, Lemma 2.1.2].

The morphism β associates to any Ω-point of $H_{g,n}$ the Ω-point of the configuration space $\mathbb{P}^{|B|}$ determined by the branch locus of the associated cover. More specifically, β associates to any cover $\phi_\Omega : X_\Omega \to \mathbb{P}^1_\Omega$ the Ω-point $[a_0 : \ldots : a_{|B|}]$ of $\mathbb{P}^{|B|}$ where a_i are the coefficients of the polynomial whose roots are the branch points of ϕ_Ω. Note that the k-points of the image of β correspond to polynomials with no multiple roots.

We denote by $\mathcal{H}_{g,n}$ the image $\tau(H_{g,n})$ in $\mathcal{M}_g$. Given a smooth connected k-curve X, then X corresponds to a point of $\mathcal{H}_{g,n}$ if and only if there exists a subgroup $G \subset \mathrm{Aut}(X)$ with quotient $X/G \simeq \mathbb{P}^1$. Note that $\mathcal{H}_{g,1}$ is simply the locus $\mathcal{H}_g$ of hyperelliptic curves in $\mathcal{M}_g$.

It is often more useful to describe the branch locus of ϕ_Ω directly as an Ω-point of $(\mathbb{P}^1)^{|B|}$. This can be done by considering an ordering of the branch points of ϕ_Ω. The branch locus of a cover corresponding to a k-point of $H_{g,n}$ can be any k-point of $(\mathbb{P}^1)^{|B|} - \Delta$ where Δ is the weak diagonal consisting of points having at least two equal coordinates. In particular, for any Ω-point $(b_1, \ldots, b_{2g+2})$ of $(\mathbb{P}^1)^{2g+2} - \Delta$ there is a unique hyperelliptic cover $\phi_\Omega : X_\Omega \to \mathbb{P}^1_\Omega$ branched at $\{b_1, \ldots, b_{2g+2}\}$. Also the curve X_Ω has genus g.

3.2. The fibres of $H_{g,n}$

We now describe some properties of a G-Galois cover $\phi : X \to \mathbb{P}^1$ corresponding to a point of $H_{g,n}$. In fact, the cover ϕ arises as the fibre product of n hyperelliptic covers which satisfy a strong disjointness condition on their branch loci.

Consider an isomorphism $\iota : (\mathbb{Z}/2)^n \simeq G$. For $i \in \{1, \ldots, n\}$, this isomorphism determines a natural element s_i of order 2 in G. Let $H_i \simeq (\mathbb{Z}/2)^{n-1}$ be the subgroup generated by all s_j for $j \neq i$. Suppose for $i \in \{1, \ldots, n\}$ that B_i is a non-empty finite subset of $\mathbb{P}^1$ of even cardinality. For any non-empty $S \subset \{1, \ldots, n\}$, denote by B_S the set of all $b \in \mathbb{P}^1$ such that $b \in B_i$ for an odd number of $i \in S$ and denote by $C_S \to \mathbb{P}^1$ the hyperelliptic cover branched at B_S. Finally, let H_S be the subgroup of G consisting of all elements $\sum_{i=1}^n a_i s_i$ such that $\sum_{i \in S} a_i$ is even. Note that each H_S is non-canonically isomorphic to $(\mathbb{Z}/2)^{n-1}$. Furthermore, when $S = \{i\}$ we have $B_S = B_i$ and $H_S = H_i$.

Lemma 2. *Suppose $\phi : X \to \mathbb{P}^1$ is the normalized fibre product over $\mathbb{P}^1$ of n smooth hyperelliptic covers $C_i \to \mathbb{P}^1$ with branch loci B_i. Then ϕ is a G-Galois cover and the quotient of X by H_S is the hyperelliptic cover $C_S \to \mathbb{P}^1$ branched at B_S.*

Proof. The cover $\phi : X \to \mathbb{P}^1$ is a G-Galois cover of (possibly disconnected) smooth curves by the definition of the fibre product. Also by definition, $C_i \to \mathbb{P}^1$ is the quotient of X by the subgroup H_i.

The branch locus B of ϕ equals $\cup_{i=1}^n B_i$. For $b \in B$, the inertia group I_b of $X \to \mathbb{P}^1$ above b must be cyclic; thus $I_b \simeq \mathbb{Z}/2$. In fact, the generator $(\alpha_1, \ldots, \alpha_n)$ of I_b satisfies $\alpha_i = 1$ if and only if $b \in B_i$. To see this, note that if $b \in B_i$, then $C_i \to \mathbb{P}^1$ is branched at b and so $I_b \not\subset H_i$; it follows that $\alpha_i = 1$ if $b \in B_i$. On the other hand, if $b \notin B_i$, then $C_i \to \mathbb{P}^1$ is unramified at b and so $I_b \subset H_i$; it follows that $\alpha_i = 0$ if $b \notin B_i$.

Since $H_S \simeq (\mathbb{Z}/2)^{n-1}$, the quotient $X/H_S \to \mathbb{P}^1$ is hyperelliptic; it remains to show that the branch locus of this cover is B_S. For $b \in B$, the cover $X/H_S \to \mathbb{P}^1$ is branched at b if and only if $I_b \not\subset H_S$, which is equivalent to $(\alpha_1, \ldots, \alpha_n) \notin H_S$. So $X/H_S \to \mathbb{P}^1$ is branched at b if and only if $\Sigma_{i \in S} \alpha_i$ is odd. Now, $\Sigma_{i \in S} \alpha_i \equiv \#\{i \in S | b \in B_i\}$ mod 2, so this number is odd if and only if $b \in B_i$ for an odd number of $i \in S$. Thus X/H_S is branched at B_S by definition.

In Section 5, we construct covers $\phi : X \to \mathbb{P}^1$ corresponding to points of $H_{g,n}$ for which X is also hyperelliptic. For example, when $n = 2$, suppose ϕ is the normalized fibre product of two hyperelliptic covers ϕ_1 and ϕ_2. The curve X will also be hyperelliptic if its quotient $C_{1,2} = X/H_{1,2}$ is isomorphic to $\mathbb{P}^1$. This occurs when $g_1 = g_2$ and B_1 and B_2 overlap in all but one point; or when $g_2 = g_1 + 1$ and $B_1 \subset B_2$. The other extreme is considered in [14] where Stepanov uses the fibre product of two hyperelliptic curves whose branch loci intersect in a single point to construct Goppa codes.

We say that the collection $\{B_i\}_{i=1}^n$ is *strongly disjoint* if the following two conditions are satisfied: first, the sets B_S are distinct for all non-empty $S \subset \{1, \ldots, n\}$; second, $B = \cup_{i=1}^n B_i$ is a simple horizontal divisor. In other words, if $b_1, b_2 \in B$ are two Ω-points of $\mathbb{P}^1_\Omega$ for some scheme Ω, then the second condition insures that either $b_1 = b_2$ or that b_1 and b_2 do not intersect in $\mathbb{P}^1_\Omega$.

Lemma 3. *A cover $\phi : X \to \mathbb{P}^1$ corresponds to a point of $H_{g,n}$ if and only if X has genus g and $\phi : X \to \mathbb{P}^1$ is isomorphic to the normalized fibre product over $\mathbb{P}^1$ of n smooth hyperelliptic covers $C_i \to \mathbb{P}^1$ whose branch loci B_i form a strongly disjoint set.*

Proof. If $\phi : X \to \mathbb{P}^1$ is the normalized fibre product of n hyperelliptic covers with branch loci B_i, then it is clear that ϕ is a G-Galois cover and X is projective. Furthermore, $C_j \to \mathbb{P}^1$ is disjoint from the normalized fibre product of all $C_i \to \mathbb{P}^1$ for $i \leq j$; otherwise, by Lemma 2, $C_j \to \mathbb{P}^1$ would be isomorphic to $C_S \to \mathbb{P}^1$ for some $\{j\} \neq S \subset \{1, \ldots, n\}$. This would imply $B_S = B_j$ for some $S \neq \{j\}$ which would contradict the fact that $\{B_i\}$ form a strongly disjoint set. Since these covers are disjoint over $\mathbb{P}^1$, it follows that X is connected. Also X is a smooth relative curve since $B = \cup_{i=1}^n B_i$ is a simple horizontal divisor. By hypothesis, X has genus g and so ϕ corresponds to a point of $H_{g,n}$.

Conversely, if $\phi : X \to \mathbb{P}^1$ corresponds to a point of $H_{g,n}$, then X has genus g by definition. Consider the quotients $C_i \to \mathbb{P}^1_k$ of ϕ by the subgroups H_i of G for $i = 1, \ldots, n$. These covers are clearly smooth and hyperelliptic. By the universal property of fibre products, there is a morphism from X to the normalized fibre product of the covers $C_i \to \mathbb{P}^1$. This morphism must be an isomorphism since both X and the normalized fibre product have degree 2^n over $\mathbb{P}^1$. Also, $\phi : X \to \mathbb{P}^1$ dominates the fibre product of any two of the quotients $C_S \to \mathbb{P}^1$ with branch locus B_S, by Lemma 2. Since X is connected, these quotients $C_S \to \mathbb{P}^1$ must all be disjoint; in other words, the sets B_S must all be distinct. Also, $\cup_{i=1}^n B_i$ is the branch locus B of ϕ; by definition, B is a simple horizontal divisor. Thus $\{B_i\}$ form a strongly disjoint set.

Corollary 1. *For $n \geq 2$, the locus $\mathcal{H}_{g,n}$ has dimension $(g+2^n-1)/2^{n-2}-3$ if $g \equiv 1 \bmod 2^{n-2}$ and is empty otherwise. In particular, the dimension of the locus $\mathcal{H}_{g,2}$ is g.*

Proof. The dimension of $H_{g,n}$ is equal to the dimension of $(\mathbb{P}^1)^{|B|}$, namely the number of branch points $|B|$ of the corresponding covers. By the Riemann-Hurwitz formula, $|B| = (g+2^n-1)/2^{n-2}$. By Lemma 1, the dimension of $\mathcal{H}_{g,n}$ is three less than the dimension of $H_{g,n}$, which simplifies to g when $n=2$.

3.3. Decomposition of the Jacobian

We will now describe the isogeny class of the Jacobian for any curve X for which there exists a cover $\phi : X \to \mathbb{P}^1_k$ corresponding to a k-point of $H_{g,n}$. For $i \in \{1,\dots,n\}$, suppose $\phi_i : C_i \to \mathbb{P}^1_k$ is a smooth hyperelliptic cover with branch locus B_i. Suppose $\{B_i\}_{i=1}^n$ form a strongly disjoint set and let $B = \cup_{i=1}^n B_i$.

Proposition 3. *Suppose $\phi : X \to \mathbb{P}^1_k$ is the normalization of the fibre product of ϕ_i for $i = 1,\dots,n$. Then $\mathrm{Jac}(X)$ is isogenous to $\prod(\mathrm{Jac}(C_S))$ where the product is taken over all non-empty $S \subset \{1,\dots,n\}$.*

Proof. Note that X/H_S is the hyperelliptic curve C_S by Lemma 2. Thus the result follows directly from [8, Theorem C] if $\mathrm{genus}(X) = \Sigma_S \,\mathrm{genus}(C_S)$. By the Riemann-Hurwitz formula, $\mathrm{genus}(C_S) = -1+|B_S|/2$. Since $B = \cup_{i=1}^n B_i$ is the branch locus of $X \to \mathbb{P}^1_k$, it follows that $\mathrm{genus}(X) = 2^{n-2}|B| - 2^n + 1$. The proof follows by showing that $\Sigma_S |B_S| = 2^{n-1}|B|$ by the inclusion-exclusion principle.

The isogeny between $\mathrm{Jac}(X)$ and $\prod(\mathrm{Jac}(C_S))$ is not sufficient to study the a-number of X since the a-number is not an isogeny invariant. For this reason, we now generalize Proposition 3 by showing that the de Rham cohomology group $H^1_{\mathrm{dR}}(X)$ also decomposes. Equivalently, one could work with the crystalline cohomology group $H^1_{\mathrm{crys}}(X)$ evaluated at k, [6, 1.3.6]. We thank Kani [7] for helping us with the proof of Proposition 4. Let $N = 2^n - 1$.

Proposition 4. *Suppose $\mathrm{char}(k) \neq 2$. Then $H^1_{\mathrm{dR}}(X)$ is isomorphic to $\oplus_S H^1_{\mathrm{dR}}(C_S)$ as $k[G]$-modules, where the sum is taken over all non-empty $S \subset \{1,\dots,n\}$.*

Proof. Since $\mathrm{char}(k) \neq 2$, there exists an idempotent ε_S corresponding to the subgroup H_S in the group ring $k[G]$ for every nonempty subset $S \subset \{1,\dots,n\}$. Namely, $\varepsilon_S = \sum h/2^{n-1}$, where the sum ranges over all $h \in H_S$. Let ε_G be the idempotent $\sum h/2^n$, where the sum ranges over all $h \in G$. By Lemma 2, C_S is the quotient of X by H_S, so $H^1_{\mathrm{dR}}(C_S) \cong (H^1_{\mathrm{dR}}(X))^{H_S} \cong \varepsilon_S H^1_{\mathrm{dR}}(X)$. Furthermore, note that $0 = H^1_{\mathrm{dR}}(\mathbb{P}^1_k) \cong (H^1_{\mathrm{dR}}(X))^G \cong \varepsilon_G H^1_{\mathrm{dR}}(X)$ and therefore that $\varepsilon_G x = 0$ for all x.

If S and T are distinct subsets then $\varepsilon_S \varepsilon_T = 2^{2-2n} \sum h_s h_t$ where the sum ranges over all $h_s \in H_S$ and $h_t \in H_T$. For each $g \in G$, we see that $g h_s^{-1} \in H_T$ for half of the values of $h_s \in H_S$. So g appears 2^{n-2} times in $\sum h_s h_t$. Thus, $2^{2n-2}\varepsilon_S \varepsilon_T = 2^{n-2} \sum_{g \in G} g$ and we obtain that $\varepsilon_S \varepsilon_T = \varepsilon_G$. Similarly, one can show for all subsets S that $\varepsilon_S \varepsilon_S = \varepsilon_S$ and $\varepsilon_S \varepsilon_G = \varepsilon_G$.

We construct an explicit homomorphism γ from $\oplus_S H^1_{\mathrm{dR}}(C_S)$ to $H^1_{\mathrm{dR}}(X)$:

$$\gamma(x_1, x_2, \ldots, x_N) = \sum_{i=1}^{N} x_i.$$

If ψ is the homomorphism from $H^1_{\mathrm{dR}}(X)$ to $\oplus_S H^1_{\mathrm{dR}}(C_S)$ given by

$$\psi(y) = (\varepsilon_1 y, \varepsilon_2 y, \ldots, \varepsilon_N y)$$

then one can check that $\psi \circ \gamma = \gamma \circ \psi = \mathrm{Id}$. Thus γ is an isomorphism of k-vector spaces. In fact, γ is a $k[G]$-module isomorphism since every $g \in G$ commutes with ε_S and thus with γ.

The following corollary will be used throughout the remainder of the paper.

Corollary 2. *Suppose* $\mathrm{char}(k) > 2$. *There is an isomorphism between* $\mathrm{Jac}(X)[p]$ *and* $\prod_S(\mathrm{Jac}(C_S)[p])$ *as group schemes where the product is taken over all non-empty* $S \subset \{1, \ldots, n\}$. *In particular,* $\mathrm{Jac}(X)$ *and* $\prod_S(\mathrm{Jac}(C_S))$ *have the same p-rank and a-number.*

Proof. By Proposition 4, there is an isomorphism of k-vector spaces between $H^1_{\mathrm{dR}}(X)$ and $\oplus_S H^1_{\mathrm{dR}}(C_S)$. By the functoriality of the Frobenius and Verschiebung morphisms, F and V commute with the action of $g \in G$ and thus with the idempotents ε_S. It follows that $H^1_{\mathrm{dR}}(X)$ and $\oplus_S H^1_{\mathrm{dR}}(C_S)$ are naturally isomorphic as $k[V,F]$-modules. Since X and C_S are smooth curves, [5, 3.11.2] implies that $H^1_{\mathrm{dR}}(\mathrm{Jac}(X))$ and $\oplus_S H^1_{\mathrm{dR}}(\mathrm{Jac}(C_S))$ are isomorphic as $k[V,F]$-modules. By [9, 5.11], $H^1_{\mathrm{dR}}(\mathrm{Jac}(X))$ is canonically isomorphic to the contravariant Dieudonné module associated to $\mathrm{Jac}(X)[p]$. Likewise, $H^1_{\mathrm{dR}}(\mathrm{Jac}(C_S)))$ is canonically isomorphic to the contravariant Dieudonné module associated to $\mathrm{Jac}(C_S)[p]$. So the Dieudonné module of $\mathrm{Jac}(X)[p]$ is isomorphic to the direct sum of the Dieudonné modules of $\mathrm{Jac}(C_S)[p]$. It follows, from the equivalence of categories between finite commutative group schemes over k and their contravariant Dieudonné modules, that the group schemes $\mathrm{Jac}(X)[p]$ and $\prod_S(\mathrm{Jac}(C_S)[p])$ are isomorphic.

4. Configurations of non-ordinary hyperelliptic curves

The results in this section will be used to find curves X having interesting p-power torsion, as measured in terms of invariants such as the p-rank and a-number. Corollary 2 shows that when a cover $\phi : X \to \mathbb{P}^1$ corresponds to a point of $H_{g,n}$ then such invariants for X can be determined by the corresponding invariants of its $\mathbb{Z}/2$-quotients. Since these quotients are all hyperelliptic, one can apply results of Yui [17]. The main difficulty is to control the p-torsion of all of the curves C_S in terms of the p-torsion of the curves C_i.

Let C be a smooth hyperelliptic curve of genus g defined over an algebraically closed field k of characteristic $p > 2$. Recall that C admits a $\mathbb{Z}/2$-Galois cover $\phi_1 : C \to \mathbb{P}^1_k$ with $2g+2$ distinct branch points. Without loss of generality, we suppose ϕ_1 is branched at ∞ and choose an equation for this cover of the form

$y^2 = f(x)$, where $f(x)$ is a polynomial of degree $2g+1$. We denote the roots of $f(x)$ by $\{\lambda_1, \dots, \lambda_{2g+1}\}$.

Denote by c_r the coefficient of x^r in the expansion of $f(x)^{(p-1)/2}$. Then

$$c_r = (-1)^{r-(p-1)/2} \sum \binom{(p-1)/2}{a_1} \cdots \binom{(p-1)/2}{a_{2g+1}} \lambda_1^{a_1} \cdots \lambda_{2g+1}^{a_{2g+1}} \qquad (1)$$

where the sum ranges over all $2g+1$-tuples $(a_1, \dots, a_{2g+1})$ of integers such that $0 \le a_i \le (p-1)/2$ for all i and $\sum a_i = (2g+1)(p-1)/2 - r$. Note that c_r can be viewed as a polynomial in $k[\lambda_1, \dots, \lambda_{2g+1}]$ which is homogeneous of degree $(2g+1)(p-1)/2 - r$ and which is of degree $(p-1)/2$ in each variable.

Let A_g be the $g \times g$ matrix whose ijth entry is c_{ip-j}. The determinant of A_g defines a polynomial in $k[\lambda_1, \dots, \lambda_{2g+1}]$ which we denote by $\mathrm{Det}_g(\lambda_1, \dots, \lambda_{2g+1}) = \mathrm{Det}_g(\underline{\lambda}_{2g+1})$. This polynomial is of degree at most $g(p-1)/2$ in each λ_i and is homogeneous of total degree $g^2(p-1)/2$. It is invariant under the action of S_{2g+1} on the variables λ_i. We denote by $D_g \subset (\mathbb{A}^1_k)^{2g+1}$ the hypersurface of points $\underline{\lambda}_{2g+1} = (\lambda_1, \dots, \lambda_{2g+1})$ for which $\mathrm{Det}_g(\underline{\lambda}_{2g+1}) = 0$.

In [17], Yui gives the following characterization of non-ordinary hyperelliptic curves. Recall that Δ is the weak diagonal consisting of points with at least two equal coordinates.

Theorem 2. *(*Yui [17]*) Suppose C is a smooth hyperelliptic curve of genus g. Then C is non-ordinary if and only if there is a $\mathbb{Z}/2$-Galois cover $\phi : C \to \mathbb{P}^1_k$ branched at ∞ and at $2g+1$ distinct points $\lambda_i \in \mathbb{A}^1_k$ such that $\underline{\lambda}_{2g+1} \in D_g$.*

We now find some results on the geometry of the hypersurface D_g which will be used in Sections 5 and 6 to construct curves in $\mathcal{H}_{g,n}$ whose p-torsion has prescribed invariants. In Lemma 4 and Lemma 5, we show that $\mathrm{Det}_g(\underline{\lambda}_{2g+1})$ is generically a polynomial of degree $d = g(p-1)/2$ in the variable λ_{2g+1} whose roots are not contained in $\{\lambda_1, \dots, \lambda_{2g}\}$. We expect for a generic choice of $\lambda_1, \dots, \lambda_{2g}$ that this polynomial will have d distinct roots. Showing this seems to be related to the question of whether the hyperelliptic locus is transversal (in the strict geometric sense) to the locus $V_{g,g-1}$ of nonordinary curves. So in Proposition 5, we instead prove the weaker statement that this polynomial has at least $(p-1)/2$ distinct roots.

Lemma 4. *The determinant* $\mathrm{Det}_g(\underline{\lambda}_{2g+1})$ *is a polynomial of degree $d = g(p-1)/2$ in the variable λ_{2g+1}.*

Proof. As we observed above, the degree of $\mathrm{Det}_g(\underline{\lambda}_{2g+1})$ in λ_{2g+1} is at most d. We claim that the coefficient of λ_{2g+1}^d is a non-zero polynomial in $k[\lambda_1, \dots, \lambda_{2g}]$. In particular, one term of this polynomial is $(-1)^{g(p-1)/2} \lambda_{2g+1}^d \prod_{i=1}^{2g} \lambda_i^{(g - \lceil i/2 \rceil)(p-1)/2}$.

To see this, we note first from Equation 1 that the total degree of c_{gp-j} is $(2g+1)(p-1)/2 - (gp-j) = (p-1)/2 + (j-g)$. So if $j < g$ then $\lambda_{2g+1}^{(p-1)/2}$ cannot appear in c_{gp-j}. Furthermore, the coefficient of $\lambda_{2g+1}^{(p-1)/2}$ in c_{gp-g} is exactly $(-1)^{(p-1)/2}$. Because the degree of λ_{2g+1} in c_r is at most $(p-1)/2$ for all r, a monomial in $\mathrm{Det}_g(\underline{\lambda}_{2g+1})$ will be divisible by λ_{2g+1}^d only if it is the product of matrix entries which are each divisible by $\lambda_{2g+1}^{(p-1)/2}$. Thus c_{gp-g} is the only entry in the bottom row of A_g which contributes to the terms of $\mathrm{Det}_g(\lambda_{2g+1})$ which are divisible by λ_{2g+1}^d.

Similarly, in the penultimate row of A_g, the total degree of $c_{(g-1)p-j}$ will be $3(p-1)/2+(j-(g-1))$. Therefore, if $j<g-1$ then $(\lambda_1\lambda_2\lambda_{2g+1})^{(p-1)/2}$ cannot divide $c_{(g-1)p-j}$. Because the degree of λ_1 for all c_r in A_g is at most $(p-1)/2$, only the last two entries of the penultimate row contribute to the terms of $\mathrm{Det}_g(\lambda_{2g+1})$ which are divisible by $\lambda_1^{(g-1)(p-1)/2}$. Also the coefficient of $(\lambda_1\lambda_2\lambda_{2g+1})^{(p-1)/2}$ in $c_{(g-1)p-(g-1)}$ is $(-1)^{(p-1)/2}$.

Continuing, we see that only terms which are on or above the diagonal can contribute to the desired term of $\mathrm{Det}_g(\lambda_{2g+1})$. It follows that the only term of $\mathrm{Det}_g(\lambda_{2g+1})$ which involves the monomial $\lambda_{2g+1}^d\prod_{i=1}^{2g}\lambda_i^{(g-\lceil i/2\rceil)(p-1)/2}$ comes from the product of elements of the diagonal. The coefficient of this monomial is the product of g coefficients which each equal $(-1)^{(p-1)/2}$, so it is equal to $(-1)^{g(p-1)/2}$.

Lemma 5. *The image of* $\mathrm{Det}_g(\lambda_{2g+1})$ *in* $k[\lambda_1,\dots,\lambda_{2g+1}]/(\lambda_{2g+1}-\lambda_1)$ *is non-constant.*

Proof. The proof is similar to that of Lemma 4. It is sufficient to show that at least one of the coefficients of $\mathrm{Det}_g(\lambda_1,\dots,\lambda_{2g},\lambda_1)$ is non-zero. The coefficient of the monomial $\lambda_1^{g(p-1)/2}\prod_{i=1}^{2g}\lambda_i^{(g-\lceil i/2\rceil)(p-1)/2}$ is $2(-1)^{g(p-1)/2}$ as this monomial appears exactly twice as the product of terms in the diagonal of the Hasse-Witt matrix and does not appear again in the expansion of the determinant.

Suppose exactly two branch points of a smooth hyperelliptic cover specialize together. The resulting curve is singular and consists of a hyperelliptic curve C' of genus $g-1$ self-intersecting in a point. The geometric interpretation of the next lemma is that this singular curve will be ordinary if and only if C' is ordinary.

Lemma 6. $\mathrm{Det}_g(\lambda_1,\dots,\lambda_{2g-1},0,0)=(-\lambda_1\cdots\lambda_{2g-1})^{(p-1)/2}\,\mathrm{Det}_{g-1}(\lambda_1,\dots,\lambda_{2g-1})$.

Proof. Suppose $\lambda_{2g}=\lambda_{2g+1}=0$. Then the only nonzero terms in the sum defining c_r are those where $a_{2g}=a_{2g+1}=0$. If $r=p-1$, then the only term in this sum that does not vanish is the one where $a_i=(p-1)/2$ for $1\le i\le 2g-1$. Thus $c_{p-1}=(-\lambda_1\cdots\lambda_{2g-1})^{(p-1)/2}$. If $r<p-1$, then all of the terms in the sum are zero, and thus $c_r=0$. Suppose $r>p-1$ and $r=ip-j$. Then the term c_r occuring in the ith row and jth column of A_g equals the term $c_{r-(p-1)}$ occuring in the $(i-1)$st row and $(j-1)$st column of A_{g-1}. By expanding the determinant along the first row, we see that $\mathrm{Det}_g(\lambda_1,\dots,\lambda_{2g-1},0,0)=c_{p-1}\,\mathrm{Det}(A_{g-1})$.

For fixed $\lambda_{2g}=(\lambda_1,\dots,\lambda_{2g})\subset(\mathbb{A}_k^1)^{2g}$, denote by $L(\lambda_{2g})$ the line consisting of points $(\lambda_1,\dots,\lambda_{2g},\lambda_{2g+1})\subset(\mathbb{A}_k^1)^{2g+1}$ (where only the last coordinate varies). Generically, the intersection of $L(\lambda_{2g})$ and D_g consists of $d=g(p-1)/2$ points when counted with multiplicity. To see this, consider $\mathrm{Det}(\lambda_{2g+1})$ as a polynomial in $R[\lambda_{2g+1}]$ where $R=k[\lambda_1,\dots,\lambda_{2g}]$. The coefficient of λ_{2g+1}^d in $\mathrm{Det}(\lambda_{2g+1})$ is non-zero in R by Lemma 4. Since k is an algebraically closed field, for any $\lambda_{2g}=(\lambda_1,\dots,\lambda_{2g})$ not in the Zariski closed set of $(\mathbb{A}_k^1)^{2g}$ defined by this coefficient, $\mathrm{Det}(\lambda_{2g+1})$ has degree d and thus d roots in k when counted with multiplicity. The next proposition gives a lower bound on the number of distinct roots.

Proposition 5. *Let $U_g \subset (\mathbb{A}^1_k)^{2g}$ be the set of points $(\lambda_1,\ldots,\lambda_{2g})$ for which $L(\lambda_{2g})$ intersects D_g in at least $(p-1)/2$ non-zero distinct points of $(\mathbb{A}^1_k)^{2g+1}\backslash\Delta$. Then U_g is a nonempty Zariski open subset of $(\mathbb{A}^1_k)^{2g}$.*

Proof. The proof is by induction on g. A result of Igusa [4] states that there are exactly $(p-1)/2$ distinct values λ so that the elliptic curve branched at $\{0,1,\infty,\lambda\}$ is non-ordinary. It follows that the result is true when $g=1$.

Suppose that U_{g-1} is a nonempty Zariski open subset of $(\mathbb{A}^1_k)^{2g-2}$. First we show that for a generic choice of $(\lambda_1,\ldots,\lambda_{2g})$ there are at least $(p-1)/2$ distinct choices of λ_{2g+1} so that $\mathrm{Det}_g(\lambda_1,\ldots,\lambda_{2g},\lambda_{2g+1})=0$. It will suffice to construct a single choice of $(\lambda_1,\ldots,\lambda_{2g})$ for which this result holds, as the generic case will have at least as many distinct roots as any specialized case. It follows from Lemma 6 that for non-zero $\lambda_3,\ldots,\lambda_{2g}$, the non-zero values of λ_{2g+1} so that $\mathrm{Det}_g(0,0,\lambda_3,\ldots,\lambda_{2g},\lambda_{2g+1})=0$ and $\mathrm{Det}_{g-1}(\lambda_3,\ldots,\lambda_{2g+1})=0$ are the same. By the inductive hypothesis, for the generic choice of $(\lambda_3,\ldots,\lambda_{2g})$ there are at least $(p-1)/2$ non-zero distinct values of λ_{2g+1} with this property.

Next we show that generically these $(p-1)/2$ intersection points of $L(\lambda_{2g})$ and D_g are not contained in Δ. By Lemma 5 and by symmetry, for each $1\le i\le 2g$, the value λ_i is a root of the polynomial $\mathrm{Det}_g(\lambda_1,\ldots,\lambda_{2g+1})\in R[\lambda_{2g+1}]$ only when $(\lambda_1,\ldots,\lambda_{2g})$ is in a Zariski closed subset of $(\mathbb{A}^1)^{2g}$. So for the generic choice of $(\lambda_1,\ldots,\lambda_{2g})$, the root λ_{2g+1} will not be contained in $\{\lambda_1,\ldots,\lambda_{2g}\}$. It follows that for the generic choice of $(\lambda_1,\ldots,\lambda_{2g})$ the line $L(\lambda_{2g})$ intersects D_g in at least $(p-1)/2$ non-zero distinct points of $(\mathbb{A}^1_k)^{2g+1}\backslash\Delta$. So U_g is a nonempty Zariski open subset of $(\mathbb{A}^1_k)^{2g}$.

Proposition 6. *Let $U_g \subseteq (\mathbb{A}^1_k)^{2g}$ be defined as in Proposition 5. Then we have that $U_g\cap(D_{g-1}\times\mathbb{A}^1_k)$ has codimension 1 in $(\mathbb{A}^1_k)^{2g}$.*

Proof. Since $D_{g-1}\times\mathbb{A}^1_k$ has codimension 1 in $(\mathbb{A}^1)^{2g}$ and U_g is open by Proposition 5, it is sufficient to show that no component V of $D_{g-1}\times\mathbb{A}^1_k$ is contained in the complement W_g of U_g. Note that the complement of U_g is a Zariski closed subset defined by equations which are each symmetric in the variables $\lambda_1,\ldots,\lambda_{2g}$. On the other hand, any component V of $D_{g-1}\times\mathbb{A}^1_k$ is defined by equations that do not involve λ_{2g}. Since the ideal of W_g is not contained in the ideal of V, it follows that V is not contained in W_g.

5. Curves with prescribed *a*-number

We now consider the a-number of Jacobians of curves with commuting involutions. Recall that the a-number, $\dim_k \mathrm{Hom}(\alpha_p,\mathrm{Jac}(X))$, of a k-curve X is an integer between 0 and g. Here α_p is the kernel of Frobenius on $\mathbb{G}_a$. A generic curve is ordinary and thus has a-number equal to zero. A supersingular elliptic curve E has a-number equal to one and in this case there is a non-split exact sequence $0\to\alpha_p\to E[p]\to\alpha_p\to 0$. There is a unique isomorphism type of group scheme for the p-torsion of a supersingular elliptic curve, which we denote M. In this section we construct curves X so that $\mathrm{Jac}(X)[p]$ contains multiple copies of the group scheme M and thus has large a-number.

Let $T_{g,a}$ denote the sublocus of $\overline{\mathcal{M}}_g$ consisting of curves of genus g with a-number at least a. The codimension of $T_{g,a}$ in $\mathcal{M}_g$ is at least a since $T_{g,a} \subset V_{g,g-a}$. It is not known whether (for all g and all $0 \leq a \leq g$) there exists a curve of genus g with a-number equal to a. The results in this section give some evidence for a positive answer to this question.

We note that these results can be viewed as a generalization of [11, Section 5]. In that paper, Oort considers curves X of genus $g = 3$ with a group action by $G = (\mathbb{Z}/2)^2$ so that the three $\mathbb{Z}/2$-quotients of X are all elliptic curves. He shows that there exist (nonhyperelliptic) curves of genus 3 with a-number 3 for all primes $p \geq 3$ as well as hyperelliptic supersingular curves of genus 3 with a-number 3 for all $p \equiv 3 \bmod 4$.

Lemma 7. *The generic geometric point of the hyperelliptic locus $\mathcal{H}_g$ has a-number equal to* 0*. The non-ordinary locus has codimension one in $\mathcal{H}_g$ and its generic geometric point has a-number* 1 *and p-rank $g-1$.*

Proof. This is immediate from Theorem 1 and the fact that a curve with p-rank $g-1$ has a-number 1.

The next theorem will lead immediately to Corollary 3 which is the main result in this paper on the a-number of curves.

Theorem 3. *Suppose $n \geq 2$ and $p \geq 2n+1$. Suppose g is such that $g \equiv 1 \bmod 2^{n-2}$ and $g \geq (n-1)2^{n-2}+1$. There exists a family of smooth curves X of genus g of dimension at least $(g+2^n-1)/2^{n-2}-3-n$ so that $\mathrm{Jac}(X)[p]$ contains the group scheme M^n.*

For the proof of Theorem 3, we will construct a fibre product $\phi : X \to \mathbb{P}^1$ of n hyperelliptic covers ϕ_i so that the disjoint union of any two of the branch loci B_i will consist of exactly two points. It follows that the curves $C_{i,j}$ will have genus zero.

Proof. Write $g = 1 + \ell 2^{n-2}$. If $\ell \not\equiv n \bmod 2$, let $g_1 = (\ell+3-n)/2$. Note that $g_1 \geq 1$. By Proposition 5 and Lemma 7, as long as $n \leq (p-1)/2$, there is a Zariski open subset U_{g_1} of $(\mathbb{A}^1_k)^{2g_1}$ with the following property: there are at least n choices $\eta_1, \dots, \eta_n$ for λ_{2g_1+1} such that the corresponding hyperelliptic curve C_i is non-ordinary. By Theorem 1, after replacing U_{g_1} with a smaller Zariski open subset of $(\mathbb{A}^1_k)^{2g_1}$, we can further suppose that the curves $C_1, \dots, C_n$ will have p-rank $g_1 - 1$. Thus $\mathrm{Jac}(C_i)[p]$ contains M.

Let $\phi_i : C_i \to \mathbb{P}^1$ for $1 \leq i \leq n$ be the hyperelliptic U_{g_1}-curves corresponding to these choices. Let $\phi : X \to \mathbb{P}^1$ be the normalization of the fibre product of the covers ϕ_i. Note that X is branched at $B = \{\infty, \lambda_1, \dots, \lambda_{2g_1}, \eta_1, \dots, \eta_n\}$. By Proposition 3, the genus of X will be $2^{n-2}(2g_1+1+n) - 2^n + 1 = g$. By Corollary 2, $\mathrm{Jac}(X)[p]$ contains $\oplus_{i=1}^n \mathrm{Jac}(C_i)[p]$ which contains $\oplus_{i=1}^n M$. The dimension of this family of curves is $2g_1 - 2 = |B| - 3 - n$ which equals $(g+2^n-1)/2^{n-2} - 3 - n$. Note that the p-rank of X is at least $n(g_1-1)$.

Alternatively, if $\ell \equiv n \bmod 2$, let $g_1 = (\ell+2-n)/2$ and note $g_1 \geq 1$. By Proposition 6, the locus $U_{g_1+1} \cap (D_{g_1} \times \mathbb{A}^1_\ell)$ has codimension 1 in $(\mathbb{A}^1_k)^{2g_1+2}$. In other words, as long as $n \leq 1+(p-1)/2$, for any $(\lambda_1,\ldots,\lambda_{2g_1+2})$ in a codimension 1 subset Z of $(\mathbb{A}^1_k)^{2g_1+2}$, it is true that $(\lambda_1,\ldots,\lambda_{2g_1+1}) \in D_{g_1}$ and there are at least $n-1$ choices η_i of λ_{2g_1+3} with $(\lambda_1,\ldots,\lambda_{2g_1+3}) \in D_{g_1+1}$. Let $\phi_n : C_n \to \mathbb{P}^1$ be the hyperelliptic cover branched at $(\lambda_1,\ldots,\lambda_{2g_1+1})$. For $1 \leq i \leq n-1$, let $\phi_i : C_i \to \mathbb{P}^1$ be the hyperelliptic cover branched at $(\lambda_1,\ldots,\lambda_{2g_1+2},\eta_i)$. Then C_n has genus g_1 and C_i has genus g_1+1 for $1 \leq i \leq n-1$. By Theorem 1, after restricting to a Zariski open subset of Z, we can further suppose that C_n (resp. C_i) has p-rank g_1-1 (resp. g_1). Thus $\mathrm{Jac}(C_i)[p]$ contains M for $1 \leq i \leq n$.

Let $\phi : X \to \mathbb{P}^1$ be the normalization of the fibre product of ϕ_i for $1 \leq i \leq n$. Note that ϕ is branched at $B = \{\infty,\lambda_1,\ldots,\lambda_{2g_1+2},\eta_1,\ldots,\eta_{n-1}\}$. As above, X has genus $2^{n-2}(2g_1+2+n)-2^n+1 = g$ and $\mathrm{Jac}(X)[p]$ contains M^n. By Proposition 6, the locus Z has dimension $2g_1+1$. The corresponding family of curves has dimension $2g_1-1 = |B|-3-n$ which again equals $(g+2^n-1)/2^{n-2}-3-n$. Note that the p-rank of X is at least ng_1-1.

Corollary 3. *Suppose $n \geq 2$ and $p \geq 2n+1$. Suppose g is such that $\mathcal{H}_{g,n}$ is non-empty of dimension at least $n+1$. Then the intersection $\mathcal{H}_{g,n} \cap T_{g,n}$ has codimension at most n in $\mathcal{H}_{g,n}$. In particular, there exists a smooth curve of genus g with a-number at least n.*

Proof. By Corollary 1, the condition that $\mathcal{H}_{g,n}$ is non-empty is equivalent to $g \equiv 1 \bmod 2^{n-2}$ and the condition that $\mathcal{H}_{g,n}$ has dimension at least $n+1$ is equivalent to $g \geq (n-1)2^{n-2}+1$. The family constructed in Theorem 3 has dimension $(g+2^n-1)/2^{n-2}-3-n$ and thus codimension n in $\mathcal{H}_{g,n}$. For any fibre X in this family, $\mathrm{Jac}(X)[p]$ contains M^n and so X has a-number at least n. So this family is contained in $\mathcal{H}_{g,n} \cap T_{g,n}$.

When $n=2$ or $n=3$, then the curves found in Theorem 3 are in fact hyperelliptic.

Corollary 4. *Suppose $g \geq 2$ and $p \geq 5$. There exists a $(g-2)$-dimensional family of smooth hyperelliptic curves of genus g whose fibres have a-number 2 and p-rank $g-2$.*

The family in Corollary 4 has codimension 2 in $\mathcal{H}_{g,2}$.

Proof. This follows immediately from Theorem 3 once we show that the curve X is hyperelliptic when $n=2$. If g is even, note that the branch loci of ϕ_1 and ϕ_2 differ in only one point. The third quotient $C_{1,2}$ of X by $\mathbb{Z}/2$ is branched at only two points η_1 and η_2. So the cover $X \to C_{1,2}$ is hyperelliptic. Likewise, if g is odd, then the third quotient $C_{1,2}$ of X by $\mathbb{Z}/2$ is branched at only two points λ_{2g_1+2} and η_1 so the cover $X \to C_{1,2}$ is hyperelliptic. In both cases, $\mathrm{Jac}(X)[p] \simeq \mathrm{Jac}(C_1)[p] \oplus \mathrm{Jac}(C_2)[p]$ and so the fibres of X have a-number 2 and p-rank $g-2$.

Corollary 5. *Suppose $g \geq 5$ is odd and $p \geq 7$. There exists a $(g-5)/2$-dimensional family of smooth hyperelliptic curves X of genus g so that $\mathrm{Jac}(X)[p]$ contains M^3 and thus has a-number at least 3.*

The family in Corollary 5 has codimension 3 in $\mathcal{H}_{g,3}$.

Proof. It is sufficient to show that the fibres of the family constructed in Theorem 3 are hyperelliptic when $n = 3$. In both cases of the construction, if $S = \{1,2\}$, $\{1,3\}$, or $\{2,3\}$, then the quotient $C_S \to \mathbb{P}^1$ of X by $H_S \simeq (\mathbb{Z}/2)^2$ is branched at only two points and so C_S has genus 0. Consider the quotient X' of X by the subgroup $H' \simeq \mathbb{Z}/2$ generated by $h = (1,1,1)$. Note that X' dominates C_S if $S = \{1,2\}$, $\{1,3\}$, or $\{2,3\}$, since $h \in H_S$. It follows that X' has genus zero since $X' \to \mathbb{P}^1$ is a $(\mathbb{Z}/2)^2$-cover having three $\mathbb{Z}/2$-quotients of genus zero. It follows that $X \to X'$ is hyperelliptic.

Remark 1. One would like to strengthen Corollary 5 by producing curves with a-number exactly 3. The difficulty is to determine the a-number of $C_{\{1,2,3\}}$. For example, to construct a curve of genus $g = 5$ and a-number exactly 3 with this method, one would need to guarantee that there are supersingular values λ_1, λ_2 and λ_3 so that the hyperelliptic curve of genus two branched at $\{0,1,\infty,\lambda_1,\lambda_2,\lambda_3\}$ is ordinary.

Remark 2. In the above results, some restriction on p is unavoidable. By Proposition 3.1 of [13], there does not exist a hyperelliptic curve of genus 2 and a-number 2 when $p = 3$ or of genus 3 and a-number 3 when $p = 3$ or 5. Also, there does not exist a hyperelliptic curve with a-number 4 when $g = 4$ and $p = 3,5$ or when $g = 5$ and $p = 3$.

We now produce curves of every genus with a-number at least 4 using this method. (One can also produce curves of every genus with a-number at least 3 and count the dimension of these families). The curves constructed in this way will most likely not be hyperelliptic. This makes it difficult to produce a curve of every genus with every possible a-number using induction and fibre products.

Corollary 6. *Suppose $g \geq 7$ and $p \geq 5$. There exists a curve of genus g with a-number at least* 4*.*

Proof. If g is even, let $g_1 = g/2$. Note that $g_1 - 2 \geq 2$. From Corollary 4, there exists a hyperelliptic curve of genus $g_1 - 2$ and a-number 2. Consider the corresponding hyperelliptic cover ϕ_1 branched at $\{\lambda_1,\ldots,\lambda_{2g_1-3},\infty\}$. Consider a hyperelliptic cover ϕ_2 branched at $\{\eta_1,\ldots,\eta_5,\infty\}$ which has a-number 2. After modifying ϕ_2 by an affine linear transformation, one can suppose that $\{\eta_i\} \cap \{\lambda_i\}$ is empty. The cardinality of $(B_1 \cup B_2)\backslash(B_1 \cap B_2)$ is $(2g_1 - 2) + 6 - 2 = 2g_1 + 2$. It follows from Proposition 3 that the fiber product of ϕ_1 and ϕ_2 yields a curve with genus $(g_1 - 2) + g_1 + 2 = g$ and a-number at least 4.

If g is odd, let $g_1 = (g-1)/2$. Note that $g_1 - 1 \geq 2$. By Corollary 4, there exists a hyperelliptic curve of genus $g_1 - 1$ and a-number 2. Consider the corresponding hyperelliptic cover ϕ_1 branched at $\{\lambda_1,\ldots,\lambda_{2g_1-2},0,\infty\}$. Consider a hyperelliptic cover ϕ_2 branched at $\{\eta_1,\ldots,\eta_4,0,\infty\}$ which has a-number 2. After modifying ϕ_2 by a scalar transformation, one can suppose that $\{\eta_i\} \cap \{\lambda_i\}$ is empty. The cardinality of $(B_1 \cup B_2)\backslash(B_1 \cap B_2)$ is $2g_1 + 6 - 4 = 2g_1 + 2$. It follows from Proposition 3 that the fiber product of ϕ_1 and ϕ_2 yields a curve with genus $(g_1 - 1) + g_1 + 2 = g$ and a-number at least 4.

6. Curves with prescribed p-torsion

The methods of the previous sections can also be used to construct Jacobians whose p-torsion contains group schemes other than μ_p or α_p. In this section, we illustrate this for two particular isomorphism types of group scheme, namely the p-torsion of a supersingular abelian surface which is not superspecial and of a supersingular abelian variety of dimension 3 with a-number 1.

Section 3 allows one to describe the p-torsion of the Jacobian of a curve X which corresponds to a point of $\mathcal{H}_{g,n}$. Specifically, Proposition 4 states that $\mathrm{Jac}(X)[p]$ is the direct sum of $\mathrm{Jac}(C_S)[p]$ where C_S is the quotient of X by H_S and S ranges over the $2^n - 1$ nonempty subsets of $\{1, \dots, n\}$. With this method, it is only possible to construct Jacobians so that $\mathrm{Jac}(X)[p]$ is decomposable into (at least two) group schemes each of which occurs as the p-torsion of a hyperelliptic curve.

Via the p-rank, we have already considered the group scheme for the p-torsion of an ordinary elliptic curve, namely $\mathbb{Z}/p \oplus \mu_p$. Using the a-number, we have already studied the group scheme M of the p-torsion of a supersingular elliptic curve.

Not many other group schemes are known to occur as the p-torsion of a hyperelliptic curve. There are four possibilities of group scheme which occur among curves of genus 2 (which are automatically hyperelliptic). The first three $(\mathbb{Z}_p \oplus \mu_p)^2$, $(\mathbb{Z}/p \oplus \mu_p) \oplus M$, and M^2 are decomposable. We will focus on the most interesting of the four, namely the group scheme N for the p-torsion of a supersingular abelian surface which is not superspecial. A curve X with $\mathrm{Jac}(X)[p] \simeq N$ has genus 2 and is thus hyperelliptic.

By [3, Example A.3.15], there is a filtration $H_1 \subset H_2 \subset N$ where $H_1 \simeq \alpha_p$, $H_2/H_1 \simeq \alpha_p \oplus \alpha_p$ and $N/H_2 \simeq \alpha_p$. Moreover, the kernel G_1 of Frobenius and the kernel G_2 of Verschiebung are contained in H_2 and there is an exact sequence $0 \to H_1 \to G_1 \oplus G_2 \to H_2 \to 0$.

The group scheme N is perhaps easier to describe in terms of its covariant Dieudonné module. Consider the non-commutative ring $E = W(k)[F,V]$ with the Frobenius automorphism $\sigma : W(k) \to W(k)$ and the relations $FV = VF = p$ and $F\lambda = \lambda^{\sigma} F$ and $\lambda V = V \lambda^{\sigma}$ for all $\lambda \in W(k)$. Recall that there is an equivalence of categories between finite commutative group schemes $\mathbb{G}$ over k (with order p^r) and finite left E-modules $D(\mathbb{G})$ (having length r as a $W(k)$-module), see for example [3, A.5]. By [3, Example A.5.1-5.4], $D(\mu_p) = k/k(V, 1-F)$, $D(\alpha_p) = k/k(F,V)$, and $D(N) = k/k(F^3, V^3, F^2 - V^2)$.

The p-rank of a curve X with $\mathrm{Jac}(X)[p] \simeq N$ is zero. To see this, note that $\mathrm{Hom}(\mu_p, N) = 0$ or that F and V are both nilpotent on $D(N)$. The a-number of a curve X with $\mathrm{Jac}(X)[p] \simeq N$ is one. (It is at least one since the p-rank is 0 and at most one since the abelian surface is not superspecial.) This also follows from the structure of the group scheme or from the fact that $N[F] \cap N[V] = H_1 \simeq \alpha_p$.

Lemma 8. *There is a one-dimensional family of smooth curves X of genus two with* $\mathrm{Jac}(X)[p] \simeq N$.

Proof. The dimension in $\mathcal{A}_2$ of supersingular (resp. superspecial) abelian surfaces is one (resp. zero). It follows that the locus of abelian surfaces with p-torsion N is exactly one. The generic point of this one-dimensional family must be in the image of the Torelli morphism since $\overline{\mathcal{M}}_2$ and $\overline{\mathcal{A}}_2$ have the same dimension. So there is a one-dimensional family of curves of genus two with p-rank 0 and a-number 1. The fibres of this family are all smooth since the family cannot intersect either of the boundary components Δ_0 or Δ_1.

Lemma 9. *There exists a one-dimensional family of smooth hyperelliptic curves X of genus 3 with $\mathrm{Jac}(X)[p] \simeq N \oplus (\mathbb{Z}/p \oplus \mu_p)$.*

Proof. By Lemma 8, there is a one-dimensional family of smooth curves X of genus two with $\mathrm{Jac}(X)[p] \simeq N$. This yields a family of hyperelliptic covers of $\mathbb{P}^1$ branched at six points. For some subset of four of these points, the family of elliptic curves branched at these points must have varying j-invariant and so its fibres are generically ordinary. The fibre product of these two families of covers yields a family of smooth hyperelliptic curves of genus 3 with p-torsion $N \oplus (\mathbb{Z}/p \oplus \mu_p)$ by Corollary 2.

The following proposition will be used to generalize Lemma 9 for $g \geq 4$.

Proposition 7. *Suppose there exists an r-dimensional family of smooth hyperelliptic curves C of genus g' with $\mathrm{Jac}(C)[p] \simeq \mathbb{G}$ for some group scheme $\mathbb{G}$. Suppose $s \geq 1$ and $g = 2g' - 1 + s$. Then there exists an $(r+s)$-dimensional family of smooth curves X in $\mathcal{H}_{g,2}$ so that $\mathrm{Jac}(X)[p]$ contains $\mathbb{G}$.*

Proof. For each curve C in the original family with $\mathrm{Jac}(C)[p] \simeq \mathbb{G}$ and branch locus $B_0 = \{\lambda_1, \dots, \lambda_{2g'+2}\}$, we will construct an s-dimensional family of smooth curves X so that $\mathrm{Jac}(X)[p]$ contains $\mathbb{G}$. By Proposition 3 and Lemma 2, it will suffice to construct hyperelliptic curves C_1 and C_2 whose branch loci B_1 and B_2 are of even cardinality with $|B_1 \cap B_2| = s$ and $B_0 = (B_1 \cup B_2) \backslash (B_1 \cap B_2)$.

If $s = 2m$ is even, then $B_1 = B_0 \cup \{\eta_1, \dots, \eta_{2m}\}$ and $B_2 = \{\eta_1, \dots, \eta_{2m}\}$ satisfy these restrictions and there are $2m = s$ choices for the points η_i. Similarly, if $s = 2m+1$ is odd, then we can set $B_1 = \{\lambda_1, \dots, \lambda_{2g'+1}, \eta_1, \dots, \eta_{2m+1}\}$ and $B_2 = \{\lambda_{2g'+2}, \eta_1, \dots, \eta_{2m+1}\}$ satisfy these restrictions. There are $2m+1 = s$ choices for η_i. The Jacobian of the normalized fibre product X of C_1 and C_2 contains $\mathrm{Jac}(C)$.

This is the main result of the section.

Corollary 7. *Let N be the p-torsion of a supersingular abelian surface which is not superspecial. For all $g \geq 2$, there exists a smooth hyperelliptic curve X so that $\mathrm{Jac}(X)[p]$ contains N.*

Proof. The statement will follow from induction. Assume for all g' such that $2^n \leq g' < 2^{n+1}$ that there exists a smooth hyperelliptic curve $X_{g'}$ so that $\mathrm{Jac}(X_{g'})[p]$ contains N. This is true for $n = 1$ by Lemma 8 and Lemma 9. If $2^{n+1} \leq g < 2^{n+2}$, then $g = 2g'$ or $g = 2g' + 1$ for some g' such that $2^n \leq g' < 2^{n+1}$. Using Proposition 7 with $s = 1$ or $s = 2$ allows one to construct a curve X_g of genus g so that $\mathrm{Jac}(X_g)[p]$ contains N. If $s = 1$ or $s = 2$ in Proposition 7, then B_2 consists of exactly two points so X_g is also hyperelliptic.

Similarly, one can consider the group scheme Q of the p-torsion of a supersingular abelian variety of dimension three with a-number 1. A curve X with $\mathrm{Jac}(X)[p] = Q$ has p-rank 0. Also, $D(Q) = k[F,V]/k(F^4, V^4, F^3 - V^3)$. The restriction on g in the next corollary could be removed if there exists a smooth hyperelliptic curve X of genus 4 so that $\mathrm{Jac}(X)[p]$ contains Q.

Corollary 8. *Let Q be the p-torsion of a supersingular abelian variety of dimension three with a-number 1. Suppose $g \geq 3$ is not a power of two. Then there exists a smooth hyperelliptic curve X of genus g so that $\mathrm{Jac}(X)[p]$ contains Q.*

Proof. The proof parallels that of Corollary 7. One starts with the supersingular hyperelliptic curve X of genus 3 and a-number 1 (and thus $\mathrm{Jac}(X)[p] \simeq Q$) from [11] and works inductively using Proposition 7.

It is natural to ask whether Corollary 7 could be strengthened to state that $\mathrm{Jac}(X)[p] \simeq N \oplus (\mathbb{Z}/p \oplus \mu_p)^{g-2}$. This raises the following geometric question.

Question 1. Given any choice of $\Lambda = \{\lambda_1, \dots, \lambda_{2r}\}$, does there exist $\mu \in \mathbb{A}^1_k - \Lambda$ so that the hyperelliptic curve branched at $\{\lambda_1, \dots, \lambda_{2r}, \mu, \infty\}$ is ordinary?

For a generic choice of Λ, the answer to Question 1 is yes by Lemma 4. This question will have an affirmative answer if the hypersurface D_r does not contain any coordinate line $L(\lambda_{2r})$. The question is equivalent to asking whether, given a hyperelliptic cover $\phi : X \to \mathbb{P}^1_k$, it is always possible to deform X to an ordinary curve by moving only one branch point.

An affirmative answer to Question 1 would allow one to strengthen Proposition 7 to state that $\mathrm{Jac}(X)[p] \simeq \mathbb{G} \oplus (\mathbb{Z}/p \oplus \mu_p)^{g'-1+s}$. This is because the curves C_1 and C_2 in the proof can be generically chosen to be ordinary. So an affirmative answer to Question 1 would imply that for all $g \geq 4$ there exists a smooth hyperelliptic curve X with $\mathrm{Jac}(X)[p] \simeq N \oplus (\mathbb{Z}/p \oplus \mu_p)^{g-2}$. If this is true, then $\mathrm{Jac}(X)[p] \simeq N \oplus (\mathbb{Z}/p \oplus \mu_p)^{g-2}$ when X is the generic geometric point of $\mathcal{H}_g \cap V_{g,g-2}$.

Acknowledgements. We would like to thank E. Goren for suggesting the topic of this paper, E. Kani for help with Proposition 4, and J. Achter, I. Bouw, F. Oort, and the referee for helpful comments.

References

[1] C. Faber and G. van der Geer. Complete subvarieties of moduli spaces and the Prym map. *J. Reine Angew. Math.*, 573:117–137, 2004.

[2] D. Glass and R. Pries. Questions on p-torsion of hyperelliptic curves. Workshop on automorphisms of curves, Leiden, August 2004.

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

[4] J.-I. Igusa. Class number of a definite quaternion with prime discriminant. *Proc. Nat. Acad. Sci. U.S.A.*, 44:312–314, 1958.

[5] L. Illusie. Complexe de de Rham-Witt et cohomologie cristalline. *Ann. Sci. École Norm. Sup. (4)*, 12(4):501–661, 1979.

[6] L. Illusie. Crystalline cohomology. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 43–70. Amer. Math. Soc., Providence, RI, 1994.

[7] E. Kani. Personal communication.

[8] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284(2):307–327, 1989.

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

[10] F. Oort. Subvarieties of moduli spaces. *Invent. Math.*, 24:95–119, 1974.

[11] F. Oort. Hyperelliptic supersingular curves. In *Arithmetic algebraic geometry (Texel, 1989)*, volume 89 of *Progr. Math.*, pages 247–284. Birkhäuser Boston, Boston, MA, 1991.

[12] R. Pries. Families of wildly ramified covers of curves. *Amer. J. Math.*, 124(4):737–768, 2002.

[13] R. Re. The rank of the Cartier operator and linear systems on curves. *J. Algebra*, 236(1):80–92, 2001.

[14] S. Stepanov. Fibre products, character sums, and geometric Goppa codes. In *Number theory and its applications (Ankara, 1996)*, volume 204 of *Lecture Notes in Pure and Appl. Math.*, pages 227–259. Dekker, New York, 1999.

[15] H. Völklein. *Groups as Galois groups*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1996.

[16] S. Wewers. Construction of Hurwitz spaces. Thesis.

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