HYPERELLIPTIC CURVES WITH a-NUMBER 1 IN SMALL CHARACTERISTIC

ARSEN ELKIN AND RACHEL PRIES

ABSTRACT. For every $g \geq 3$, we show there exists a hyperelliptic curve of genus g with p-rank g-3 and a-number 1 in characteristic p when p=3 or p=5. The method of proof is to show that a generic point of the moduli space of hyperelliptic curves of genus 3 and p-rank 0 has a-number 1. When p=3, we also show that this moduli space is irreducible.

1. Introduction

Suppose X is a curve of genus g defined over an algebraically closed field k of characteristic p. The p-torsion of the Jacobian $\operatorname{Jac}(X)$ can be studied using invariants such as the p-rank σ_X and a-number a_X . In Section 2, we define these invariants. Briefly, the p-rank of X is $\sigma_X = \dim_{\mathbb{F}_p} \operatorname{Hom}(\mu_p, \operatorname{Jac}(X))$ where the group scheme μ_p is the kernel of Frobenius on \mathbb{G}_m . The a-number of X is $a_X = \dim_k \operatorname{Hom}(\alpha_p, \operatorname{Jac}(X))$ where the group scheme α_p is the kernel of Frobenius on \mathbb{G}_a . It is well known that σ_X, a_X are non-negative integers with $0 \le \sigma_X + a_X \le g$.

There are many open problems about the p-rank and a-number of curves. In some sense this is surprising, since there are algorithms to compute the p-rank and the a-number of X for a given prime p and a given curve X. However, these algorithms are not well-suited for proving existence results for curves of arbitrary genus in arbitrary characteristic. For this reason, many of the existence results on this topic are non-constructive and rely on deep theorems from arithmetic geometry, e.g., [2, Thm. 2.3].

A result from [8] is that, for every prime p and every $g \ge 3$, there exists a k-curve X of genus g with p-rank g-3 and a-number 1. The author also gives a strategy for extending this result to the case of hyperelliptic curves and explains some of the difficulties involved with this strategy. In this paper, we carry out this strategy when p=3 and p=5, which yields the following result (found in Section 4).

Corollary 1.1. Suppose $g \ge 3$. Let p = 3 or p = 5. Then there exists a hyperelliptic curve of genus g in characteristic p with p-rank g - 3 and a-number 1.

For the proof, we consider the moduli space $\mathcal{H}_3 \cap V_{3,0}$ whose points correspond to hyperelliptic curves of genus 3 with p-rank 0. When p=3 and p=5, we give an explicit proof that every generic point of this moduli space has a-number 1 in Section 3. This provides the base case of an inductive process found in [8]. Using induction on g, we conclude that the locus of curves having a-number 1 is an open and dense subspace of the moduli space of hyperelliptic curves of genus g and g-rank g-3 (Theorem 4.2).

We also show that $\mathcal{H}_3 \cap V_{3,0}$ is irreducible when p = 3 (Proposition 3.5). It is an open question whether $\mathcal{H}_3 \cap V_0$ is irreducible when p > 3. We describe the computational complexity of this problem in Section 3.4.

The second author was partially supported by NSF grant DMS-07-01303. We thank J. Achter for his comments on drafts of this paper.

2. Invariants of the p-torsion of Jacobians

2.1. The *p*-rank and *a*-number. Throughout the paper, we work over an algebraically closed field k of characteristic p. The group scheme μ_p is the kernel of Frobenius on \mathbb{G}_m and the group scheme α_p is the kernel of Frobenius on \mathbb{G}_a . As schemes, $\mu_p \simeq \operatorname{Spec}(k[x]/(x-1)^p)$ and $\alpha_p \simeq \operatorname{Spec}(k[x]/x^p)$. See [4, A.3] for more details about these group schemes.

Suppose X is a smooth projective k-curve of genus g with Jacobian Jac(X). The p-rank of X is $\sigma_X = \dim_{\mathbb{F}_p} \operatorname{Hom}(\mu_p, \operatorname{Jac}(X))$ and the a-number of X is $a_X = \dim_k \operatorname{Hom}(\alpha_p, \operatorname{Jac}(X))$. The p-rank is the integer σ_X such that the number of p-torsion points of $\operatorname{Jac}(X)$ is p^{σ_X} . It is well-known that $0 \le \sigma_X + a_X \le g$.

2.2. Moduli spaces of curves with given invariants. Let \mathcal{M}_g denote the moduli space of smooth projective curves of genus g defined over k. Let $\mathcal{H}_g \subset \mathcal{M}_g$ denote the sublocus consisting of hyperelliptic curves. The dimension of \mathcal{H}_g is 2g-1. Let $V_{g,\sigma} \subset \mathcal{M}_g$ denote the closed sublocus consisting of curves of genus g with p-rank at most σ . Every irreducible component of $\mathcal{H}_g \cap V_{g,\sigma}$ has dimension $g-1+\sigma$ by [3, Thm. 1].

Let $T_{g,2} \subset \mathcal{M}_g$ denote the closed sublocus of curves with a-number at least 2. Recall that $T_{g,2} \subset V_{g,g-2}$. If $g \geq 2$ and $\sigma = g-2$, the generic point of every irreducible component of $\mathcal{H}_g \cap V_{g,g-2}$ has a-number 1, [8, Thm. 4.1]. It follows that $\dim(\mathcal{H}_g \cap T_{g,2}) \leq 2g-4$. In particular, $\dim(\mathcal{H}_3 \cap T_{3,2}) \leq 2$.

- Remark 2.1. When p=2, every hyperelliptic cover is wildly ramified. As a result, the computation of the p-rank or a-number of a hyperelliptic curve differs significantly when p=2 from the case when p is odd. For example, every hyperelliptic curve of genus 3 and p-rank 0 has a-number 2 [2, 3.2]. For every finite field $\mathbb F$ of characteristic 2, and for $0 \le \sigma \le 3$, there is a formula for the number of isomorphism classes of hyperelliptic curves defined over $\mathbb F$ with genus 3 and p-rank σ [5, Table 3].
- 2.3. Computing the *p*-rank and *a*-number. Suppose that $p \geq 3$ and that X is hyperelliptic. There is a $\mathbb{Z}/2$ -Galois cover $\phi: X \to \mathbb{P}^1_k$ with 2g+2 distinct branch points. Without loss of generality, we suppose ϕ is branched at ∞ and choose an affine equation for ϕ of the form $y^2 = f(x)$, where $f(x) \in k[x]$ is a polynomial of degree 2g+1.

Let c_s denote the coefficient of x^s in the expansion of $f(x)^{(p-1)/2}$. For $0 \le \ell \le g-1$, let A_ℓ be the $g \times g$ matrix whose ijth entry is $(c_{ip-j})^{p^\ell}$. The matrix A_0 is the Hasse-Witt matrix of X. The Cartier-Manin matrix is $M = (\prod_{\ell=0}^{g-1} A_\ell)$.

Lemma 2.2. Suppose X is a hyperelliptic curve of genus g with equation $y^2 = f(x)$ as above.

- (1) The a-number of X is $a_X = g r$ where r is the rank of A_0 .
- (2) The p-rank of X is $\sigma_X = \text{rank}(M)$.

Proof. The Hasse-Witt matrix of X is the matrix for the action of Frobenius on $H^1(X, \mathcal{O}_X)$. By duality, one can consider the matrix of the Cartier operator on $H^0(X, \Omega_X^1)$ instead. The result then follows from [11].

Remark 2.3. It is a general phenomenon that $a_X = 0$ occurs only when $\sigma_X = g$ [6, p.416]. Lemma 2.2 illustrates this for hyperelliptic curves: if $a_X = 0$ then A_0 is invertible, and thus M is invertible, which implies that $\sigma_X = g$.

3. Hyperelliptic curves of genus 3

3.1. Parametrization of hyperelliptic curves of genus 3. Let Y be a smooth hyperelliptic curve of genus 3. Then Y has an affine equation $y^2 = f(x)$ where $f(x) \in k[x]$ has distinct roots and is of degree 7. We say that the equation $y^2 = f(x)$ is in standard form if $f(x) = x^7 + ax^6 + bx^5 + cx^4 + dx^3 + ex^2 + x$ for some $a, b, c, d, e \in k$.

Lemma 3.1. Every smooth hyperelliptic curve Y of genus 3 has an affine equation $y^2 = f(x)$ in standard form. There are only finitely many choices of f(x) so that $y^2 = f(x)$ is an affine equation in standard form for Y.

Proof. If Y is hyperelliptic then there is a morphism $\phi: Y \to \mathbb{P}^1_k$ of degree 2. If Y has genus 3 then the Riemann-Hurwitz formula implies that the branch locus B of ϕ contains exactly 8 points. After a change of coordinates on \mathbb{P}^1_k , we can suppose $0, \infty \in B$. Then ϕ is given by an affine equation of the form $y^2 = f(x)$ for some $f(x) \in k[x]$ with $\deg(f(x)) = 7$ and f(0) = 0. Write $f(x) = \sum_{i=1}^7 a_i x^i$ where $a_i \in k$ and $a_1 a_7 \neq 0$.

Consider a change of coordinates $T(y) = \alpha y$ and $T(x) = \beta x$ with $\alpha, \beta \in k$ and $\alpha\beta \neq 0$. Let $f_T(x) = (a_7\beta^7/\alpha^2)x^7 + \cdots + (a_1\beta/\alpha^2)x$. Then $y^2 = f_T(x)$ is another affine equation for Y. Let $\alpha, \beta \in k^*$ be solutions to $\alpha = (a_1^7/a_7)^{1/12}$ and $\beta = (a_1/a_7)^{1/6}$. Then the equation $y^2 = f_T(x)$ is in standard form.

Suppose $y^2 = f_1(x)$ and $y^2 = f_2(x)$ are two equations for Y in standard form. Then there is a change of coordinates $T: k[x,y]/(y^2-f_1(x)) \to k[x,y]/(y^2-f_2(x))$. Since the hyperelliptic involution is in the center of $\operatorname{Aut}(Y)$, the change of coordinates descends to an automorphism T of \mathbb{P}^1_k . Also T stabilizes $\{0,\infty\}$. After possibly composing T with an inversion $x \mapsto 1/x$, we can suppose T fixes 0 and ∞ . It follows that $T(x) = \beta x$ and $T(y) = \alpha y$ for some $\alpha, \beta \in k^*$. Then $\beta^7/\alpha^2 = \beta/\alpha^2 = 1$. Thus $\beta^6 = 1$ so there are at most 6 choices for β and for each of these there are at most 2 choices for α .

3.2. Irreducibility of $\mathcal{H}_3 \cap V_{3,0}$ when p=3. In this section, suppose p=3. The main result of the section is that $\mathcal{H}_3 \cap V_{3,0}$ is irreducible. In the next lemma, we first show that all smooth hyperelliptic curves Y of genus 3 have a-number at most 1. The lemma is a special case of [1, Thm. 1], but we include a proof for the convenience of the reader. See [10] for similar results for curves that are not hyperelliptic.

Lemma 3.2. If p = 3, then $\mathcal{H}_3 \cap T_{3,2} = \emptyset$. In other words, there are no smooth hyperelliptic curves of genus 3 with a-number at least 2.

Proof. Suppose Y is a smooth hyperelliptic curve of genus 3. By Lemma 3.1, Y has an affine equation $y^2 = f(x)$ where $f(x) = x^7 + ax^6 + bx^5 + cx^4 + dx^3 + ex^2 + x$. If p = 3, the entries of A_0 are given by the coefficients of f(x):

$$A_0 = \left(\begin{array}{ccc} e & 1 & 0 \\ b & c & d \\ 0 & 1 & a \end{array} \right).$$

If $a_Y \geq 2$, then rank $(A_0) \leq 1$ by Lemma 2.2(1). This implies e = b = d = a = 0. Then $f(x) = x(x^2 + c^{1/3}x + 1)^3$ does not have distinct roots which contradicts the hypothesis that Y is smooth. Thus $a_Y \leq 1$. П

By Lemma 3.2, every point of the two-dimensional space $\mathcal{H}_3 \cap V_{3.0}$ has a-number 1 when p=3. In fact, we can say more about the geometry of $\mathcal{H}_3 \cap V_{3,0}$ when p=3. The next result gives necessary and sufficient conditions on the five parameters a, \ldots, e for Y to have p-rank 0.

Lemma 3.3. Suppose Y is a smooth hyperelliptic curve with affine equation $y^2 =$ f(x) where $f(x) = x^7 + ax^6 + bx^5 + cx^4 + dx^3 + ex^2 + x$. Then Y has p-rank 0 in exactly the following cases:

- (1) d = 0, $a = b + c^4 = e + c^3 = 0$; (2) $d \neq 0$, $b^3 + c^{12} + c^9 a + d^3 + a^4 = d^6 e + d^6 c^3 + a^9 = d^9 c^3 + d^9 a + d^3 a^9 + a^{13} = 0$.

Proof. By Lemma 2.2(2), Y has p-rank 0 exactly when $M = A_0 A_1 A_2$ is the zero matrix. One computes that the matrix M has entries m_{ij} where:

$$\begin{split} m_{11} &= e^{13} + b^3 e^9 + b^9 e + b^9 c^3; \\ m_{12} &= e^4 + b^3 + c^9 e + c^{12} + d^3; \\ m_{13} &= d^9 e + d^9 c^3 + d^3 a^9; \\ m_{21} &= e^{12} b + e^9 c b^3 + b^{10} + b^9 c^4 + b^9 d; \\ m_{22} &= b e^3 + c b^3 + c^9 b + c^{13} + c^9 d + c d^3 + d a^3; \\ m_{23} &= d^9 b + d^9 c^4 + d^{10} + a^9 c d^3 + a^{12} d; \\ m_{31} &= b^3 e^9 + b^9 c^3 + b^9 a; \\ m_{32} &= b^3 + c^{12} + c^9 a + d^3 + a^4; \\ m_{33} &= d^9 c^3 + d^9 a + d^3 a^9 + a^{13}. \end{split}$$

Let $I \subset k[a,b,c,d,e]$ be the ideal $I = (m_{ij} \mid 1 \leq i,j \leq 3)$. Consider a point $w=(a,b,c,d,e)\in\mathbb{A}^5_k$. Let $V(I)\subset\mathbb{A}^5_k$ be the variety of I. Then Y has p-rank 0 if and only if $w \in V(I)$.

- (1) Suppose $w \in V(I)$ and d = 0. Then equation m_{33} implies a = 0. Then equation m_{32} implies $b + c^4 = 0$. If e = 0, then equation m_{11} implies c = 0and so $e + c^3 = 0$. (Note that $y^2 = x^7 + x$ is not smooth, so the case e = 0can be disregarded anyway.) If $e \neq 0$, then equation m_{12} implies $e + c^3 = 0$. Conversely, if $d = a = b + c^4 = e + c^3 = 0$, then a computer calculation shows that $w \in V(I)$.
- (2) Suppose $w \in V(I)$ and $d \neq 0$, then equation m_{13} implies $d^6e + d^6c^3 + a^9 = 0$. Also equation m_{32} implies $b^3 + c^{12} + c^9 a + d^3 + a^4 = 0$. Then equation m_{33} implies $d^9c^3 + d^9a + d^3a^9 + a^{13} = 0$. Conversely, after solving for e, b, andthen c, and substituting them into m_{ij} , a computer calculation shows that $w \in V(I)$.

Lemma 3.4. Let $I \subset k[a,b,c,d,e]$ be the ideal $I = (m_{ij} \mid 1 \leq i,j \leq 3)$ as above. Then V(I) is irreducible with dimension two.

Proof. Suppose that $(a,b,c,d,e) \in V(I)$ with $d \neq 0$. Using the equations from Lemma 3.3(2), one can solve for b and e in terms of $a^{1/3},c,d$, and then one can solve for c in terms of $a^{1/3}$ and d. Namely, $e = 2c^3 + 2a^9/d^6$ and $b = 2c^4 + 2c^3a^{1/3} + 2d + 2a^{4/3}$. Also $c = 2a^{1/3} + 2a^3/d^2 + 2a^{13/3}/d^3$. Thus there are formulae $b(a^{1/3},d)$, $c(a^{1/3},d)$, $e(a^{1/3},d)$ for b,c,e in terms of $a^{1/3},d$.

Let $S = \operatorname{Spec}(k[a^{1/3},d,d^{-1}])$. Note that S is irreducible with dimension 2. Let $C \subset \mathbb{A}^5_k$ be the closed subspace of points (a,b,c,d,e) with d=0. Let $U=\mathbb{A}^5-C$. The morphism $G((a^{1/3},d))=(a,b(a^{1/3},d),c(a^{1/3},d),d,e(a^{1/3},d))$ yields an isomorphism $G:S\to V(I)\cap U$. Thus $V(I)\cap U$ is irreducible with dimension two.

It remains to show that $V(I) \cap C$ is in the boundary of $V(I) \cap U$. Let $W \subset V(I) \cap U$ be the closed locus where $d^2 + a^2 = 0$. Recall that if $w \in V(I)$ then $d^6e + d^6c^3 + a^9 = 0$ and $(b + c^4)^3 + c^9a + d^3 + a^4 = 0$. If also $w \in W$, then $e + c^3 + a^3 = 0$. When a = d = 0, these relations imply that $e + c^3 = b + c^4 = 0$. Thus every point of $V(I) \cap C$ is in the boundary of $V(I) \cap U$.

Proposition 3.5. When p = 3, the moduli space $\mathcal{H}_3 \cap V_{3,0}$ is irreducible.

Proof. Let $\Delta \subset \mathbb{A}^5_k$ be the closed subset of all (a,b,c,d,e) so that f(x) has multiple roots. Let $U' = \mathbb{A}^5_k - \Delta$. There is a morphism $\tau : U' \to \mathcal{H}_3$ which is surjective (and finite-to-one) by Lemma 3.1. Then $\tau^{-1}(\mathcal{H}_3 \cap V_{3,0}) = V(I) \cap U'$. By Lemma 3.4, V(I) is irreducible. Thus $\mathcal{H}_3 \cap V_{3,0}$ is irreducible when p = 3.

3.3. The case when p=5. In this section, suppose p=5. The computations of the previous section become more elaborate. We show that $\mathcal{H}_3 \cap T_{3,2}$ has exactly one irreducible component of dimension two and that its generic point has p-rank 1. Using this, we show that the generic point of every irreducible component of $\mathcal{H}_3 \cap V_{3,0}$ has a-number 1.

Lemma 3.6. If p = 5, then $\mathcal{H}_3 \cap T_{3,2}$ contains exactly one irreducible component of dimension 2 and the generic point of this component has a-number 2 and p-rank 1.

Proof. If p=5, the entries of A_0 are given by some of the coefficients of $f(x)^2$:

$$A_0 = \begin{pmatrix} 2d + e^2 & 2e & 1\\ 2e + 2ad + 2bc & 2 + 2ae + c^2 + 2bd & 2cd + 2a + 2be\\ 1 & 2a & 2b + a^2 \end{pmatrix}.$$

If Y has a-number at least 2, then the rank of A_0 is at most 1. Thus the first two rows of A_0 are a non-zero scalar multiple of the third row. This implies that $(a,b,c,d,e) \in V(J)$ where $J \subset k[a,b,c,d,e]$ is the ideal (t_1,t_2,t_3,t_4) where:

$$t_1 = 4ad + 2ae^2 + 3e;$$

$$t_2 = 4bd + 2be^2 + 2a^2d + a^2e^2 + 4;$$

$$t_3 = 2ae + 4a^2d + 4abc + 3 + 4c^2 + 3bd;$$

$$t_4 = 2be + 4bad + 4b^2c + 2a^2e + 2a^3d + 2a^2bc + 3cd + 3a.$$

By equation t_1 , if a = 0 then e = 0. Then bd = -1 and c = 0. Similarly, if e = 0, then ad = 0 and bd = -1, which gives a = c = 0. In either case, this yields a component of V(J) of dimension 1.

Suppose $ae \neq 0$. Then equation t_1 implies that $d = 2e^2 + 3e/a$. After making this substitution, equation t_2 implies that $b = 2a^2 + 3a/e$. After making this substitution, equations t_3 and t_4 simplify as follows:

$$t_3' = 3a^3ce + 2a^2c + 4c^2e;$$

$$t_4' = 4ca^4e + ca^3 + ce^2a + 4ce^3.$$

If $c \neq 0$, then one can show that $c = 3a^3 + 2a^2/e$. Also $c \neq 0$ implies $ae \neq 1$. Another computation then shows that there is a relation between a and e, namely $a^3 = e^3$. Thus the intersection $V(J) \cap \{c \neq 0\}$ has dimension one, which yields a subset of $\mathcal{H}_3 \cap \mathcal{T}_{3,2}$ having dimension one.

Otherwise, if c = 0, then $t_3' = t_4' = 0$. In other words,

$$V(J) \cap \{ae \neq 0, c = 0\} = \{(a, b, 0, d, e) \mid b = 2a^2 + 3a/e, d = 2e^2 + 3e/a\}.$$

Thus there is a unique irreducible component of V(J) having dimension two. As in the proof of Proposition 3.5, there is a surjective finite-to-one morphism $\tau: U' \to \mathcal{H}_3$. Then $\tau^{-1}(\mathcal{H}_3 \cap T_{3,2}) = V(J) \cap U'$. This yields a unique irreducible component η of $\mathcal{H}_3 \cap T_{3,2}$ having dimension two.

We now find a point $w \in V(J)$ with $ae \neq 0$ and c = 0 so that the corresponding curve Y_w is a smooth hyperelliptic curve of genus 3 with a-number 2 and p-rank 1. Let $\gamma \in \mathbb{F}_{25}$ be a root of x^2-2 . Consider the point $w = (\gamma, 4+3\gamma, 0, 2+4\gamma, 1) \in V(J)$. One can compute that the discriminant of $f(x) = x^7 + \gamma x^6 + (4+3\gamma)x^5 + (2+4\gamma)x^3 + x^2 + x$ is 4 and so f(x) has distinct roots. Thus Y_w is a smooth hyperelliptic curve of genus 3. Also Y_w has a-number 2 since $w \in V(J)$. One can compute that

$$A_0(w) = \begin{pmatrix} 3\gamma & 2 & 1\\ 4\gamma + 3 & 1 + \gamma & 3 + 3\gamma\\ 1 & 2\gamma & \gamma \end{pmatrix}.$$

Thus $M = A_0 A_1 A_2$ simplifies to:

$$M(w) = \begin{pmatrix} 2\gamma & 3 & 4\\ \gamma + 2 & 4\gamma + 4 & 2\gamma + 2\\ 4 & 3\gamma & 4\gamma \end{pmatrix}.$$

Then $Y_w \in \eta$ has p-rank 1 since $\operatorname{rank}(M(w)) = 1$. The p-rank can only decrease under specialization. Thus the generic point of η has p-rank 1 and a-number 2. \square

3.4. Complexity Analysis. As the characteristic increases, the sort of analysis on the a-number and p-rank performed in previous sections becomes prohibitively complicated. To see this, let $f(x) = a_7 x^7 + a_6 x^6 + a_5 x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$. Then every coefficient of $g(x) = f(x)^{(p-1)/2}$ is homogeneous of degree (p-1)/2 when considered as a polynomial in $k[a_0, \ldots, a_7]$.

The coefficient of x^{p-1} in g(x) contains a monomial $a_2^{(p-1)/2}$. The degree in a_2 of any other coefficient of g(x) is strictly less than (p-1)/2. Thus the entry a_{11} of $A_0 = (a_{ij})$ contains a monomial $a_2^{(p-1)/2}$, and all other entries of this matrix have smaller degree as polynomials in a_2 . The non-homogeneous version of this statement is that the highest power of e appearing in the Cartier-Manin matrix for the curve $y^2 = x^7 + ax^6 + bx^5 + cx^4 + dx^3 + ex^2 + x$ appears in the monomial $e^{(p-1)/2}$ in the entry a_{11} .

This, in turn, implies that a_{11}^p contains a monomial $e^{p(p-1)/2}$, and this is the highest degree to which e appears in the entries of the matrix $A_1 = (a_{ij}^p)$. Similarly, $a_{11}^{p^2}$ contains $e^{p^2(p-1)/2}$, and the degree of e is smaller in all the other entries of $A_2 = (a_{ij}^p)$. Therefore, $e^{(1+p+p^2)(p-1)/2} = e^{(p^3-1)/2}$ is a monomial in the entry m_{11} of the product $(m_{ij}) := A_0 A_1 A_2$. A similar analysis can be performed for a_4 (or c) in the entry $m_{2,2}$ and for a_6 (or a) in the entry $m_{3,3}$.

This discussion demonstrates that the entries of the matrix A_0 , whose rank is analyzed in connection with the a-number, contain monomials of degree (p-1)/2 in a, c, and e. The entries of the matrix $A_0A_1A_2$, examined for p-rank, have the same variables appearing with degrees $(p^3-1)/2$. In particular, the locus $\mathcal{H}_3 \cap V_{3,0}$ corresponds to the vanishing of nine equations in five variables, at least three of which have degree $(p^3-1)/2$ in some variable. The difficulty of analyzing these two invariants grows accordingly.

4. Application: hyperelliptic curves with p-rank g-3 and a-number 1

Let $g \ge 3$. Suppose X is a curve of genus g with p-rank g-3. By Remark 2.3, there are three possibilities for the a-number of X, namely $a_X \in \{1, 2, 3\}$.

Remark 4.1. If X has genus g and p-rank g-3, there are four possibilities for the isomorphism class of the group scheme $\operatorname{Jac}(X)[p]$. Of these, there is a unique group scheme with p-rank g-3 and a-number 1. It is of the form $(\mathbb{Z}/p \oplus \mu_p)^{g-3} \oplus I_{3,1}$ where $I_{3,1}$ is the unique group scheme of rank 6, p-rank 0, and a-number 1. The covariant Dieudonné module for $I_{3,1}$ is $E/E(F^3-V^3)$ where E=k[F,V] is a non-commutative ring generated by Frobenius and Verschiebung [9, Lemma 3.1].

Theorem 4.2. Suppose $g \geq 3$. Let p = 3 or p = 5. Then the generic point of every irreducible component of $\mathcal{H}_q \cap V_{q,q-3}$ has a-number 1.

Proof. The proof is by induction on g with base case g=3. For p=3, $\mathcal{H}_3\cap T_{3,2}=\emptyset$ by Lemma 3.2. Thus every point of $\mathcal{H}_3\cap V_{3,0}$ has a-number 1. For p=5, there is a unique irreducible component η of $\mathcal{H}_3\cap T_{3,2}$ with dimension 2 and its generic point has p-rank 1 by Lemma 3.6. Every irreducible component ξ of $\mathcal{H}_3\cap V_{3,0}$ has dimension 2 and has generic point with p-rank 0. Thus $\xi\subsetneq T_{3,2}$. So the generic point of every irreducible component of $\mathcal{H}_3\cap V_{3,0}$ has a-number 1.

For $g \geq 4$, the result follows immediately from [8, Prop. 3.6]. Here is the basic idea of the inductive proof. The compactification $\overline{\mathcal{M}}_g$ of \mathcal{M}_g contains a boundary component Δ_0 whose generic point is a singular curve Z which self-intersects in an ordinary double point. The normalization \tilde{Z} of Z is a smooth curve of genus g-1. The p-rank of \tilde{Z} is $\sigma_{\tilde{Z}} = \sigma_Z - 1$. One proves that the closure in $\overline{\mathcal{M}}_g$ of each component of $\mathcal{H}_g \cap V_{g,g-3}$ intersects Δ_0 . Then the proof relies on a dimension count for components of Δ_0 that satisfy certain conditions on the p-rank and a-number.

Corollary 4.3. Suppose $g \ge 3$. Let p = 3 or p = 5. There is a family of dimension 2g - 4 consisting of smooth hyperelliptic curves of genus g with g-rank g - 3 and g-number g.

Proof. By Theorem 4.2, the locus of smooth hyperelliptic curves of genus g with p-rank g-3 and a-number 1 is open (and dense) in $\mathcal{H}_g \cap V_{g,g-3}$. The result follows since $\dim(\mathcal{H}_g \cap V_{g,g-3}) = 2g-4$ by [3, Thm. 1].

Remark 4.4. Here are two strategies for extending Theorem 4.2 to larger characteristic.

- (1) By [7, 5.12(4)], for all $p \geq 3$, there exists a hyperelliptic curve of genus 3 with a-number 1. The first strategy would be to see if $\mathcal{H}_3 \cap V_{3,0}$ is irreducible for all $p \geq 3$. If so, the generic point of $\mathcal{H}_3 \cap V_{3,0}$ would have a-number 1 and the result would follow from [8, Prop. 3.6].
- (2) By [3, Cor. 4], for all $p \geq 5$, there exists a hyperelliptic curve of genus 3 with a-number 2 and p-rank 1. The second strategy would be to prove that every irreducible component of $\mathcal{H}_3 \cap T_{g,2}$ of dimension two contains a point with p-rank 1. Then the generic point of every irreducible component of $\mathcal{H}_3 \cap V_{3,0}$ would have a-number 1 and the result would again follow from [8, Prop. 3.6].

References

- A. Elkin. The rank of the Cartier operator on cyclic covers of the projective line. to appear in J. Algebra, mathAG/0708.0431.
- [2] C. Faber and G. van der Geer. Complete subvarieties of moduli spaces and the Prym map. J. Reine Angew. Math., 573:117–137, 2004. arXiv:math.AG/0305334.
- [3] D. Glass and R. Pries. Hyperelliptic curves with prescribed p-torsion. Manuscripta Math., 117(3):299–317, 2005. arXiv:math.NT/0401008.
- [4] 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.
- [5] E. Nart and D. Sadornil. Hyperelliptic curves of genus three over finite fields of even characteristic. Finite Fields Appl., 10(2):198–220, 2004.
- [6] P. Norman and F. Oort. Moduli of abelian varieties. Ann. of Math. (2), 112(3):413-439, 1980.
- [7] F. Oort. Hyperelliptic supersingular curves. In Arithmetic algebraic geometry (Texel, 1989), volume 89 of Progr. Math., pages 247–284. Birkhäuser Boston, Boston, MA, 1991.
- [8] R. Pries. The p-torsion of curves with large p-rank. to appear in International Journal of Number Theory, math.AG/0601596.
- [9] R. Pries. A short guide to *p*-torsion of abelian varieties in characteristic *p*. to appear in Computational Arithmetic Geometry, CONM, AMS.
- [10] R. Re. The rank of the Cartier operator and linear systems on curves. J. Algebra, 236(1):80–92, 2001.
- [11] N. Yui. On the Jacobian varieties of hyperelliptic curves over fields of characteristic p > 2. J. Algebra, 52(2):378–410, 1978.

Arsen Elkin, Colorado State University, Fort Collins, CO, 80521, elkin@math.colostate.edu.

Rachel Pries, Colorado State University, Fort Collins, CO, 80521, pries@math.colostate.edu.