The a-number of hyperelliptic curves

Submitted by

Sarah Frei

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Master of Science

Colorado State University

Fort Collins, Colorado

Summer 2014

Master's Committee:

Advisor: Rachel Pries

Jeffery Achter
Sarah Sloane

Abstract

The a-number of hyperelliptic curves

It is known that for a smooth hyperelliptic curve to have a large a-number, the genus must be small relative to the characteristic of the field over which the curve is defined. It was proven by Elkin that for a genus g hyperelliptic curve to have $a_C = g - 1$, the genus is bounded by $g < \frac{3p}{2}$. In this paper, we show that this bound can be lowered to $g < p$ for a genus g hyperelliptic curve with $a_C = g - 1$. The method of proof is to force the Cartier-Manin matrix to have rank one and examine what restrictions that places on the affine equation defining the hyperelliptic curve. In an attempt to lower the bound further, we discuss what happens when $g = p - 1$. We then use this bound to summarize what is known about the existence of such curves when $p = 3, 5$ and 7.

Acknowledgements

I would like to thank my advisor, Dr. Rachel Pries, for her direction and constant support on this project. I have learned a tremendous amount from her about number theory as well as how to conduct research in the field of mathematics. I would also like to thank my committee members, Dr. Jeffery Achter and Dr. Sarah Sloane, for serving on my committee and for providing feedback on this paper as well as the associated presentation. Many thanks are also due to my fellow graduate students and the mathematics department at CSU for their assistance and encouragement over the past two years.

Table of Contents

List of Figures

CHAPTER 1

Introduction

Associated to an algebraic curve defined over a field of positive characteristic p are a number of invariants used to better understand the structure of the curve, such as p-rank, Newton polygon, Ekedahl-Oort type, and a-number. Knowing if and when certain properties of a curve exist gives information about the moduli space of smooth projective curves of genus g over a field k. Studied here is the a-number of hyperelliptic curves of genus g. The a-number a_C of a hyperelliptic curve C defined over an algebraically closed field k of characteristic $p > 0$ is $a_C = \dim_k \mathrm{Hom}(\alpha_p, \mathrm{Jac}(C)[p])$, where α_p is the kernel of the Frobenius endomorphism on the group scheme $\mathbb{G}_a$. While the a-number of a curve is easily computible, there are still many open questions about this invariant.

For an algebraic curve of genus g defined over $\mathbb{C}$, its Jacobian will have p^{2g} p-torsion points. However, for a curve in characteristic p, the number of p-torsion points drops to p^{f_C}, where $0 \leq f_C \leq g$. We define f_C to be the p-rank of the curve. A generic curve of genus g will have $f_C = g$. It must also be that the a-number is bounded above by $g - f_C$, so a typical curve of genus g will have $a_C = 0$. This means curves with larger a-numbers do not occur as often, and in fact curves with $a_C = g$ are very rare. An algebraic curve with $a_C = g$, called a superspecial curve, has the property that its Jacobian is isomorphic to a product of supersingular elliptic curves [Oor75]. Because superspecial curves are as far from ordinary as possible, they are a popular topic for research.

For a curve to have a large a-number, the genus of that curve must be small relative to the characteristic $p > 0$ of the field over which the curve is defined. It is a result of Ekedahl

[Eke87] that for any curve with $a_C = g$, the genus is bounded by $g \leq \frac{p(p-1)}{2}$. If the curve is hyperelliptic and $a_C = g$, then $g \leq \frac{p-1}{2}$.

If superspecial curves occur the least, then the next most infrequently occurring type of curve should be one with $a_C = g-1$. The next question that can be asked then is what kind of bound exists on the genus when $a_C = g-1$, and for any known bound, is that bound attained? It should be that the genus must still be small relative to the characteristic of the field. For a curve with $a_C = g-1$, it was shown by Re [Re01] that $g \leq p^2$. In fact, Re's results were more general, giving the bound $g \leq (g - a_C + 1)\frac{p(p-1)}{2} + p(g - a_C)$ on the genus of a curve with any a-number.

Further results by Elkin [Elk11] show that for a hyperelliptic curve with $a_C = g-1$, the bound on the genus is even lower: $g < \frac{3p}{2}$. Elkin's bound was also proven more generally, showing that if $g - a \leq \frac{2g}{p} - 2$, then there are no hyperelliptic curves of genus g with $a_C \geq a$. Work by Johnston [Joh07] confirms Elkin's bound of $g < \frac{3p}{2}$.

While these general results are useful, it is not clear whether the bound is optimal for a given a-number. The goal of this paper is to explore this bound when $a_C = g-1$ and show that it can be lowered even further. The following result is proven in Chapter 3.

THEOREM 1.0.1. *Let $g \geq p$ where p is an odd prime. Then there are no smooth hyperelliptic curves of genus g defined over a field of characteristic p with a-number equal to $g-1$.*

These results show that for a hyperelliptic curve with $a = g-1$, the bound on the genus is even lower than was previously known. We must actually have $g < p$ for such a curve to exist. Based on computations for $p = 5$ and $p = 7$, it seems possible that this bound may be even lower when $p > 3$.

When $g = p - 1$, for a genus g hyperelliptic curve to have $a = g - 1$ its affine equation $y^2 = f(x)$ must take on a particular form. It is shown in Chapter 3 that the polynomial $f(x)$ is completely determined by only three of its $2g$ coefficients.

In exploring this bound on the genus, much time was spent searching for examples of hyperelliptic curves of $g > 3$ with $a_C = g - 1$, but up to now no example has been found. It is an open question as to whether or not such curves exist, and searching for them computationally is time-consuming. Furthermore, the inability to find such a curve over small fields of definition in no way proves that they don't exist.

CHAPTER 2

Background Information

2.1. Hyperelliptic Curves and Their Jacobians

Let k be an algebraically closed field of characteristic $p > 0$. A hyperelliptic curve is a smooth curve C which is a degree 2 cover of the projective line. It can be given by an affine equation $y^2 = f(x)$ where $f(x)$ is a polynomial in $k[x]$. For C to be smooth, $f(x)$ must be squarefree. The degree of $f(x)$ determines the genus of C, where a polynomial of degree $2g+1$ or $2g+2$ corresponds to a curve of genus g. Since the automorphism group of $\mathbb{P}^1$ acts triply transitively, which means any 3 points on $\mathbb{P}^1$ can be transformed to any other 3 points by an automorphism, we are allowed to pick up to 3 of the $2g+2$ branch points of C. Hence we will always fix a branch point at infinity and $f(x)$ will be of degree $2g+1$. Often, we will also fix $x = 0$ as another branch point.

The Jacobian of a hyperelliptic curve C is a group $\mathrm{Jac}(C)$ associated to the curve. It is defined as

$$\mathrm{Jac}(C) = \frac{\mathrm{Div}^0(C)}{\mathrm{PDiv(C)}}$$

where $\mathrm{Div}^0(C)$ is the set of divisors on C of degree 0, and $\mathrm{PDiv}(C)$ is the set of principal divisors on C, that is, those that are linearly equivalent to a divisor of a meromorphic function on C.

2.2. The Cartier Operator

Let $K = k(x, y)$ be the algebraic function field of a hyperelliptic curve C given by $y^2 = f(x)$, and let $d : K \to \Omega^1(K)$ be the canonical derivation of elements in K. For a holomorphic 1-form $\omega \in H^0(C, \Omega^1_C)$, we can write it as $\omega = d\phi + \eta^p x^{p-1} dx$ with $\phi, \eta \in K$.

Definition 2.2.1. *The modified Cartier operator $C' : H^0(C, \Omega^1_C) \to H^0(C, \Omega^1_C)$ is defined for ω given as above by $C'(\omega) = \eta dx$.*

The modified Cartier operator satisfies a number of basic properties:

(1) $C'(\omega + \omega') = C'(\omega) + C'(\omega')$.

(2) $C'(\phi^p \omega) = \phi C'(\omega)$ for $\phi \in K$.

(3) $C'(\phi^{n-1}) = d\phi$ if $n = p$, and 0 otherwise for $\phi \in K$.

(4) $C'(\omega) = 0$ if and only if $\omega = d\phi$ for $\phi \in K$.

(5) $C'(\omega) = \omega$ if and only if $\omega = d\phi/\phi$ for $\phi \in K$.

All of these properties can be proven directly from the definition, except for the last, which is shown in [Car58]. For a full discussion on the Cartier operator as well as the modified Cartier operator, see [Yui78].

A canonical basis for $H^0(C, \Omega^1_C)$ is given by

$$\left\{ \omega_i = \frac{x^{i-1}dx}{y} : 1 \leq i \leq g \right\}.$$

We want to consider what the modified Cartier operator does to these basis elements. Recall that C is given by $y^2 = f(x)$, and if we let $f(x)^{(p-1)/2} = \sum_{j=0}^{N} k_j x^j$ where $N = \frac{p-1}{2}(2g+1)$, then we can rewrite ω_i as follows:

$$\begin{aligned} \omega_i =& x^{i-1} y^{-p} y^{p-1} dx = y^{-p} x^{i-1} \sum_{j=0}^{N} k_j x^j dx \\ =& y^{-p} \left(\sum_{\substack{j \\ i+j \not\equiv 0 (mod p)}} k_j x^{i+j-1} dx \right) + \sum_{l} k_{(l+1)p-i} \frac{x^{lp}}{y^p} x^{p-1} dx. \end{aligned}$$

The highest possible power of x is $N+i-1$, so $lp+p-1 \leq N+i-1$, which forces

$$0 \leq l \leq \frac{N+i}{p} - 1 = g - \frac{1}{2} - (2g+i-12p) < g - \frac{1}{2}.$$

This means the sum in the second term is over $0 \leq l \leq g-1$. Thus we can now see that

$$C'(\omega_i) = \sum_{l=0}^{g-1} k_{(l+1)p-i}^{1/p} \frac{x^l}{y} dx.$$

This shows that C' is a map on $H^0(C, \Omega_C^1)$ and we can represent it's action on the basis with a matrix. If we write $\bar{\omega} = (\omega_1, ..., \omega_g)$, then

$$C'(\bar{\omega}) = A^{(1/p)} \bar{\omega}$$

where A is a $g \times g$ matrix $[a_{ij}]$ with $a_{ij} = k_{pi-j}$.

Definition 2.2.2. *The matrix A described above is the Cartier-Manin matrix of the hyperelliptic curve C of genus g defined over k.*

2.3. P-Rank and A-Number

We first define an A-group scheme G to be a group object with the group structure described by homomorphisms on a locally free algebra A over a commutative ring R. The group structure is given by the maps $\mu : A \to A \otimes_R A$, $\varepsilon : A \to R$ and $i : A \to A$ which define the multiplication, identity, and inverse laws, respectively. For the purposes of this paper, R will be an algebraically closed field k. The group scheme $\mu_p \cong \mathrm{Spec}(k[x]/(x-1)^p)$ is the kernel of the Frobenius endomorphism on the multiplicative group $\mathbb{G}_m = \mathrm{Spec}(k[x, x^{-1}])$.

The group scheme $\alpha_p \cong \mathrm{Spec}(k[x]/x^p)$ is the kernel of the Frobenius endomorphism on the additive group $\mathbb{G}_a = \mathrm{Spec}(k[x])$. For more on group schemes, see [Tat97].

The p-rank of a hyperelliptic curve C is $f_C = \dim_k \mathrm{Hom}(\mu_p, \mathrm{Jac}(C)[p])$. An equivalent definition of the p-rank is that it is the positive integer f_C such that $\mathrm{Jac}(C)[p](k) \cong (\mathbb{Z}/p\mathbb{Z})^{f_C}$, so $\#\mathrm{Jac}(C)[p](k) = p^{f_C}$. We see that $0 \leq f_C \leq g = \dim(\mathrm{Jac}(C))$. A curve is called ordinary if $f_C = g$, and non-ordinary otherwise.

The a-number of C is $a_C = \dim_k \mathrm{Hom}(\alpha_p, \mathrm{Jac}(C)[p])$. We also have $0 \leq a_C \leq g$, and in fact $a_C \leq g - f_C$. Curves with $a_C = g$ are called superspecial and do not occur often, due to the fact that a typical curve of genus g has $f_C = g$. Curves with $a_C = g - 1$ are forced to have $f_C = 0$ or $f_C = 1$ which limits their occurrences.

The a-number is also related to the rank of the Cartier-Manin matrix introduced above. For an abelian variety X of dimension g, such as the Jacobian of a genus g hyperelliptic curve, the Frobenius operator $F : X \to X^{(p)}$ is the p-th power map on X, and the Verschiebung operator $V : X^{(p)} \to X$ is the map such that $V \circ F = [p]$, the multiplication-by-p map. The a-number is also defined [LO98] as the dimension of the kernel of the action of V on $H^0(X, \Omega^1_X)$. If we let $v = \dim V H^0(X, \Omega^1_X)$, this gives us that $a_C = g - v$. It is also known for a smooth projective curve, such as a hyperelliptic curve, C that the action of the Cartier operator on $H^0(C, \Omega^1_C)$ agrees with the action of V on $H^0(\mathrm{Jac}(C), \Omega^1_{\mathrm{Jac}(C)}) \cong H^0(C, \Omega^1_C)$ [Oda69]. Since we can express the action of the Cartier operator on $H^0(C, \Omega^1_C)$ with the Cartier-Manin matrix A, we see that $a_C = g - \mathrm{rank}(A)$.

It turns out that associated with any abelian variety X of dimension g is a short exact sequence

$$0 \to H^0(X, \Omega^1_X) \to H^1_{dR}(X) \to H^0(X, \Omega^1_X) \to 0.$$

The Frobenius operator acts on $H^0(X, \Omega^1_X)$ in this sequence, and the Verschiebung operator acts on $H^1_{dR}(X)$ so $H^0(X, \Omega^1_X) = VH^1_{dR}(X)$.

For the sake of notation, we will let $a_C = a$ for the rest of this paper. In studying hyperelliptic curves with $a = g - 1$, we will thus be looking for curves with a Cartier-Manin matrix of rank one. We will utilize the fact that for a matrix of rank 1, there is at least one non-zero entry, and every 2×2 minor has determinant 0. This ensures that all of the rows, or equivalently all of the columns, are linearly dependent.

CHAPTER 3

Results

3.1. The Case $g > p$

Example 3.1.1. Consider a genus 4 hyperelliptic curve X defined over a field of characteristic 3. It can be defined by the equation $y^2 = f(x)$. We can assume that X has a branch point at infinity, so we let

$$f(x) = x^9 + c_8x^8 + c_7x^7 + c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0.$$

Then we get the following Cartier-Manin matrix associated to X:

$$\begin{pmatrix} c_2 & c_1 & c_0 & 0 \\ c_5 & c_4 & c_3 & c_2 \\ c_8 & c_7 & c_6 & c_5 \\ 0 & 0 & 1 & c_8 \end{pmatrix}$$

If we want this matrix to have rank one, row four must be the only linearly independent row, and we get that $c_1 = c_2 = c_4 = c_5 = c_7 = c_8 = 0$. Hence f is simplified to

$$\begin{aligned} f(x) =& x^9 + c_6x^6 + c_3x^3 + c_0 \\ =& (x^3 + \sqrt[3]{c_6}x^2 + \sqrt[3]{c_3}x + \sqrt[3]{c_0})^3. \end{aligned}$$

So f is not squarefree over $\overline{\mathbb{F}}_3$. Thus over any field of characteristic 3, this hyperelliptic curve is singular, and we see that there are no smooth hyperelliptic curves of genus 4 with $a = 3$ when $p = 3$.

This example demonstrates what will always be the case when $g > p$. By forcing the Cartier-Manin matrix to have rank one, too many coefficients of $f(x)$ are forced to be 0, resulting in a polynomial with repeated roots.

For Theorems 3.1.1 and 3.2.3 we will use the following notation. Let X be a hyperelliptic curve given by the equation $y^2 = f(x)$ where $f(x) = \sum_{i=1}^{2g+1} c_i x^i$ with $c_i \in \mathbb{F}_{p^r}$ for some r. Note that by a change of variables, we can assume $c_0 = 0$ and $c_{2g+1} = 1$. We will assume that X has $a = g - 1$. Then we will define the coefficients k_i as follows:

$$f(x)^{(p-1)/2} = \sum_{i=0}^{\left(\frac{p-1}{2}\right)(2g+1)} k_i x^i$$

and $k_i = 0$ if $i < \dfrac{p-1}{2}$. The Cartier-Manin matrix A associated to X is a $g \times g$ matrix $[a_{ij}]$ where $a_{ij} = k_{pi-j}$. We will denote row m of A by A_m. For X to have a-number equal to $g - 1$, A must have rank one.

Theorem 3.1.1. *Let $g > p$ where p is an odd prime. Then there are no smooth hyperelliptic curves of genus g defined over a field of characteristic p with a-number equal to $g - 1$.*

Proof. Let $g > p$ where p is an odd prime. Since $k_i = 0$ for $0 \leq i \leq \frac{p-3}{2}$, $a_{1,j}$ is possibly nonzero for $1 \leq j \leq \frac{p+1}{2}$, and $a_{1,j} = 0$ for $\frac{p+3}{2} \leq j \leq g$. The largest nonzero term of $f(x)^{(p-1)/2}$ is $x^{g(p-1)+(p-1)/2}$, so $k_{g(p-1)+(p-1)/2} = k_{gp-(g-(p-1)/2)} = 1$ and any larger-indexed coefficient is zero. This means $a_{g,j} = 0$ for $1 \leq j \leq g - \frac{p+1}{2}$, and $a_{g,j}$ is possibly nonzero for $g - \frac{p-1}{2} \leq j \leq g$.

Now let us suppose that $g = p + m$ for some integer $m \geq 1$. We have $a_{1,(p+1)/2} = k_{(p-1)/2} = c_1^{(p-1)/2}$, and $a_{1,(p+1)/2+m} = 0$, since $a_{1,(p+1)/2}$ is the last nonzero entry in A_1. Also, $a_{g,(p+1)/2} = 0$, since $a_{g,j} = 0$ for $1 \leq j \leq g - \frac{p+1}{2} = \frac{p-1}{2} + m$ and $m \geq 1$. Hence $a_{g,(p+1)/2}$ is possibly the last zero term in A_g, if $m = 1$. Lastly, $a_{g,(p+1)/2+m} = 1$, since $g - \frac{p-1}{2} = p + m + \frac{p-1}{2} = \frac{p+1}{2} + m$, which is the first non-zero term in A_g. Using this 2×2 minor, we get $a_{1,(p+1)/2} \cdot a_{g,(p+1)/2+m} - a_{g,(p+1)/2} \cdot a_{1,(p+1)/2+m} = 0$, which forces $c_1 = 0$. But then $f(x) = \sum_{i=2}^{2g+1} c_i x^i = x^2 \sum_{i=2}^{2g+1} c_i x^{i-2}$ is not squarefree and X is not a smooth curve.

Therefore, when $g > p$ there are no smooth hyperelliptic curves of genus g defined over a field of characteristic p with a-number equal to $g - 1$. $\square$

3.2. The Case $g = p$

Before we can prove the next theorem, we need two lemmas relating the coefficients of $f(x)^{(p-1)/2}$ to the coefficients of $f(x)$. First, by the Multinomial Theorem, we see

$$\begin{aligned} f(x)^{(p-1)/2} &= (c_1 x + c_2 x^2 + ... + c_{2g} x^{2g} + x^{2g+1})^{(p-1)/2} \\ &= \sum_{m_1+m_2+...+m_{2g+1}=\frac{p-1}{2}} \binom{\frac{p-1}{2}}{m_1, m_2, \ldots, m_{2g+1}} \prod_{1 \leq t \leq 2g+1} (c_t x^t)^{m_t} \end{aligned}$$

where

$$\binom{\frac{p-1}{2}}{m_1, m_2, \ldots, m_{2g+1}} = \frac{\frac{p-1}{2}!}{m_1! m_2! \cdots m_{2g+1}!}.$$

This allows us to express each k_s in terms of the coefficients of $f(x)$:

$$k_s = \sum_{\substack{m_1+m_2+\ldots+m_{2g+1}=\frac{p-1}{2} \\ m_1+2m_2+\ldots+(2g+1)m_{2g+1}=s}} \binom{\frac{p-1}{2}}{m_1, m_2, \ldots, m_{2g+1}} \prod_{1\le t\le 2g+1} c_t^{m_t}.$$

Since $k_{\frac{p-1}{2}}$ is the first non-zero term of $f(x)^{(p-1)/2}$, we will index the first $p+1$ non-zero coefficients in terms of this one.

LEMMA 3.2.1. *Let $g = p$ and assume $c_1 \neq 0$. If $k_{\frac{p-1}{2}+i} = 0$ for some i with $2 \le i \le p-1$, and $c_j = 0$ for all j in $2 \le j \le i$, then $c_{i+1} = 0$.*

PROOF. For $k_{\frac{p-1}{2}+i}$ with i in this range and $g = p$, the coefficient can only be comprised of $f(x)$-coefficients with small indices due to the restriction that $m_1+2m_2+\ldots+(2p+1)m_{2p+1} = \frac{p-1}{2}+i$. For example,

$$k_{\frac{p-1}{2}+1} = \frac{p-1}{2} c_1^{(p-3)/2} c_2.$$

In general, for $2 \le i \le p-1$,

$$k_{\frac{p-1}{2}+i} = \sum_{\substack{m_1+m_2+\ldots+m_i=\frac{p-1}{2} \\ m_1+2m_2+\ldots+im_i=\frac{p-1}{2}+i}} \binom{\frac{p-1}{2}}{m_1, m_2, \ldots, m_i} c_1^{m_1} c_2^{m_2} \cdots c_i^{m_i} + \frac{p-1}{2} c_1^{(p-3)/2} c_{i+1}.$$

It should be noted that, while not all of the c_j, $2 \le j \le i$, occur in each term in the sum, at least one c_j must occur. That is, there cannot be a term in the sum of just c_1, because that would force $m_1 = \frac{p-1}{2}$, $m_2 = \ldots = m_i = 0$, and then $m_1 + 2m_2 + \ldots + im_i \neq \frac{p-1}{2} + i$.

If $k_{\frac{p-1}{2}+i} = 0$ and $c_j = 0$ for all j in $2 \le j \le i$, then

$$k_{\frac{p-1}{2}+i} = \frac{p-1}{2} c_1^{(p-3)/2} c_{i+1} = 0.$$

Since we are assuming $c_1 \neq 0$, we must have $c_{i+1} = 0$. $\square$

Let us continue to assume $g = p$. The last non-zero term of $f(x)^{(p-1)/2}$ is $k_{g(p-1)+(p-1)/2} = k_{(2p^2-p-1)/2}$, so we will index the last $p+1$ non-zero coefficients in terms of this one. Also, although we are assuming $c_{2g+1} = 1$, we will write it in as a coefficient to clarify over which terms we are summing.

LEMMA 3.2.2. *Let $g = p$ and assume $c_{2g+1} = c_{2p+1} \neq 0$. If $k_{(2p^2-p-1)/2-i} = 0$ for some i with $2 \leq i \leq p-1$, and $c_j = 0$ for all j in $2p-i+2 \leq j \leq 2p$, then $c_{2p-i+1} = 0$.*

PROOF. For $k_{(2p^2-p-1)/2-i}$ with i in this range and $g = p$, it can only be comprised of $f(x)$ coefficients with large indices due to the restriction that $m_1 + 2m_2 + \ldots + (2p+1)m_{2p+1} = (2p^2-p-1)/2 - i$. For example,

$$k_{(2p^2-p-1)/2-1} = \frac{p-1}{2} c_{2p} c_{2p+1}^{(p-3)/2}.$$

In general, for $2 \leq i \leq p-1$,

$$k_{(2p^2-p-1)/2-i} = \sum_{\substack{m_{2p-i+2}+\ldots+m_{2p+1}=\frac{p-1}{2} \\ \sum s m_s = (2p^2-p-1)/2-i}} \binom{\frac{p-1}{2}}{m_{2p-i+2}, \ldots, m_{2p+1}} c_{2p-i+2}^{m_{2p-i+2}} c_{2p-i+3}^{m_{2p-i+3}} \cdots c_{2p+1}^{m_{2p+1}} + \frac{p-1}{2} c_{2p-i+1} c_{2p+1}^{(p-3)/2}$$

where the lower summation is over $2p-i+2 \leq s \leq 2p+1$. Again we see that while not all of the c_j, $2p-i+2 \leq j \leq 2p$, are present in each term in the sum, at least one c_j must occur. Thus, if $k_{(2p^2-p-1)/2-i} = 0$ and $c_j = 0$ for all j in $2p-i+2 \leq j \leq 2p$, then

$$k_{(2p^2-p-1)/2-i} = \frac{p-1}{2} c_{2p-i+1} c_{2p+1}^{(p-3)/2} = 0.$$

Since we are assuming $c_{2p+1} = 1 \neq 0$, we get that $c_{2p-i+1} = 0$. $\square$

These lemmas can now be used to prove the following theorem.

THEOREM 3.2.3. *Let $g = p$ where p is an odd prime. Then there are no smooth hyperelliptic curves of genus g defined over a field of characteristic p with a-number equal to $g - 1$.*

PROOF. Let X be a hyperelliptic curve of genus g in characteristic p with $a = g - 1$. The Cartier-Manin matrix $A = [a_{i,j}]$ associated to X is as given above with $g - \frac{p+1}{2}$ zeros in A_1 and A_g. For $g = p$, this means the last $\frac{p-1}{2}$ entries of A_1 are zeros and the first $\frac{p-1}{2}$ entries of A_g are zeros. As above, $k_{\frac{p-1}{2}} = c_1^{(p-1)/2}$ and $k_{g(p-1)+(p-1)/2} = k_{(2p^2-p-1)/2} = 1$. We will assume $c_1 \neq 0$ so that X is not singular at $x = 0$. This gives us an idea of what A looks like:

$$\begin{pmatrix} k_{\frac{p-1}{2}+\frac{p-1}{2}} & \cdots & k_{\frac{p-1}{2}+1} & c_1^{(p-1)/2} & 0 & \cdots & 0 \\ & \cdots & & k_{\frac{p-1}{2}+p} & k_{\frac{p-1}{2}+(p-1)} & \cdots & k_{\frac{p-1}{2}+\frac{p+1}{2}} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{\frac{2p^2-p-1}{2}-\frac{p+1}{2}} & \cdots & k_{\frac{2p^2-p-1}{2}-(p-1)} & k_{\frac{2p^2-p-1}{2}-p} & & \cdots & \\ 0 & \cdots & 0 & 1 & k_{\frac{2p^2-p-1}{2}-1} & \cdots & k_{\frac{2p^2-p-1}{2}-\frac{p-1}{2}} \end{pmatrix}$$

Setting equal to zero the determinants of 2×2 minors involving entries in the first and second rows, we get the following relationships. When $1 \leq i \leq \frac{p-1}{2}$,

$$0 = k_{\frac{p-1}{2}+i} \cdot 1 - 0 \cdot c_1^{(p-1)/2}.$$

When $\frac{p+1}{2} \leq i \leq p-1$,

$$0 = c_1^{(p-1)/2} \cdot k_{\frac{p-1}{2}+i} - k_{\frac{p-1}{2}+p} \cdot 0.$$

Hence, $k_{\frac{p-1}{2}+i} = 0$ for $1 \leq i \leq p-1$. When we first consider $i = 1$,

$$k_{\frac{p-1}{2}+1} = \frac{p-1}{2} c_1^{(p-3)/2} c_2 = 0,$$

and we must have $c_2 = 0$. Lemma 3.2.1 then applies for $i = 2$ to show $c_3 = 0$. By reapplying lemma 3.2.1 as i increases, we get $c_j = 0$ for $4 \leq j \leq p$. Now lets consider the last two rows of C. Looking at determinants of 2×2 minors gives the following relationships. When $1 \leq i \leq \frac{p-1}{2}$,

$$0 = c_1^{(p-1)/2} \cdot k_{(2p^2-p-1)/2-i} - 1 \cdot 0.$$

When $\frac{p+1}{2} \leq i \leq p-1$,

$$0 = k_{(2p^2-p-1)/2-i} \cdot 1 - 0 \cdot k_{(2p^2-p-1)/2-p}.$$

Thus, $k_{(2p^2-p-1)/2-i} = 0$ for $1 \leq i \leq p-1$. If we first let $i = 1$,

$$k_{(2p^2-p-1)/2-1} = \frac{p-1}{2} c_{2p} c_{2p+1}^{(p-3)/2} = \frac{p-1}{2} c_{2p} = 0,$$

and we see that $c_{2p} = 0$. Now lemma 3.2.2 applies when $i = 2$ to give $c_{2p-1} = 0$. We can reapply lemma 3.2.2 as we increase i and get $c_{2p-j} = 0$ for $2 \leq j \leq p-2$. That is, $c_{p+2} = ... = c_{2p-2} = 0$.

What we see now is that most of the coefficients of $f(x)$ are zero. In fact,

$$\begin{aligned} f(x) &= x^{2p+1} + c_{p+1}x^{p+1} + c_1x \\ &= x(x^{2p} + c_{p+1}x^p + c_1) \\ &= x(x^2 + \sqrt[p]{c_{p+1}}x + \sqrt[p]{c_1})^p. \end{aligned}$$

Thus $f(x)$ is not squarefree and hence X is a singular hyperelliptic curve. Therefore, there are no smooth hyperelliptic curves of genus g defined over a field of characteristic p with a-number equal to $g-1$. $\square$

3.3. The Case $g = p - 1$

3.3.1. Examples.

Example 3.3.1. We will first show that there are no smooth hyperelliptic curves of $g = 4$ with $a = 3$ defined over a field of characteristic 5. Consider a genus 4 hyperelliptic curve X, so X is defined by $y^2 = f(x)$ where

$$f(x) = x^9 + c_8x^8 + c_7x^7 + c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x.$$

We assume that $c_0 = 0$, since a curve with $c_0 \neq 0$ is isomorphic to X with a change of variables. We get the following Cartier-Manin matrix $A = [a_{i,j}]$:

$$\begin{pmatrix} 2c_1c_3 + c_2^2 & 2c_1c_2 & c_1^2 & 0 \\ 2(c_4c_5 + c_3c_6 + c_2c_7 + c_1c_8) & 2(c_3c_5 + c_2c_6 + c_1c_7) + c_4^2 & 2(c_3c_4 + c_2c_5 + c_1c_6) & 2(c_2c_4 + c_1c_5) + c_3^2 \\ 2(c_6c_8 + c_5) + c_7^2 & 2(c_6c_7 + c_5c_8 + c_4) & 2(c_5c_7 + c_4c_8 + c_3) + c_6^2 & 2(c_5c_6 + c_4c_7 + c_3c_8 + c_2) \\ 0 & 1 & 2c_8 & 2c_7 + c_8^2 \end{pmatrix}$$

For this matrix to have rank one, we can consider 2×2 minors involving elements in the first column with $a_{4,2}$, elements in the last column with $a_{1,3}$, and elements in the middle two columns involving $a_{4,2}$ and $a_{4,3}$. These give the following relationships between the coefficients of $f(x)$:

(1) $0 = 2c_1c_3 + c_2^2$

(2) $0 = c_4c_5 + c_3c_6 + c_2c_7 + c_1c_8$

(3) $0 = 2(c_6c_8 + c_5) + c_7^2$

(4) $0 = (2(c_2c_4 + c_1c_5) + c_3^2) \cdot c_1^2$

(5) $0 = (c_5c_6 + c_4c_7 + c_3c_8 + c_2) \cdot c_1^2$

(6) $0 = (2c_7 + c_8^2) \cdot c_1^2$

(7) $4c_8(c_6c_7 + c_5c_8 + c_4) = 2(c_5c_7 + c_4c_8 + c_3) + c_6^2$

(8) $2c_8(2(c_3c_5 + c_2c_6 + c_1c_7) + c_4^2) = 2(c_3c_4 + c_2c_5 + c_1c_6)$

(9) $4c_1c_2c_8 = c_1^2$

From (9) we see that $c_1 = 4c_2c_8$ and since $c_0 = 0$, we must have $c_1 \neq 0$ so that $f(x)$ is squarefree. Hence $c_2 \neq 0$ and $c_8 \neq 0$ as well. From (1) we get $c_2 = 2c_3c_8$ and $c_3 \neq 0$. Again because $c_1 \neq 0$, equation (6) gives $c_7 = 2c_8^2$ and $c_7 \neq 0$. From (4) we see $c_3 = c_4c_8 + 4c_5c_8^2$ and from (3) we get $c_5 = 4c_6c_8 + 3c_8^4$. We can plug in what has been solved for already and write these variables in terms of c_4, c_6, and c_8:

$$c_7 = 2c_8^2$$

$$c_5 = 4c_6c_8 + 3c_8^4$$

$$c_3 = c_4c_8 + c_6c_8^3 + 2c_8^6$$

$$c_2 = 2c_4c_8^2 + 2c_6c_8^4 + 4c_8^7$$

$$c_1 = 3c_4c_8^3 + 4c_6c_8^5 + c_8^8$$

Equations (2), (5), (7) and (8) all result in the same relationship between c_4, c_6, and c_8: $0 = c_6^2 + 4c_6c_8^3 + 4c_8^6$. Hence we see that $c_6 = 3c_8^3$, and we can plug that in to simplify the expressions for the variables solved for above:

$$[c_1, c_2, c_3, c_5, c_6, c_7] = [3c_4c_8^3, 2c_4c_8^2, c_4c_8, 0, 3c_8^3, 2c_8^2]$$

This gives $f(x) = x^9 + c_8x^8 + 2c_8^2x^7 + 3c_8^3x^6 + c_4x^4 + c_4c_8x^3 + 2c_4c_8^2x^2 + 3c_4c_8^3x$, which over $\overline{\mathbb{F}}_5$ factors as

$$f(x) = x(x^3 + c_8x^2 + 2c_8^2x + 3c_8^3)(x^5 + c_4)$$

$$= x(x - 3c_8)^3(x + \sqrt[5]{c_4})^5.$$

Since $f(x)$ is not squarefree, this hyperelliptic curve is singular, and we see that there are no smooth hyperelliptic curves of genus 4 with $a = 3$ when $p = 5$.

EXAMPLE 3.3.2. We will next show that no smooth hyperelliptic curves of $g = 6$ with $a = 5$ exist over a field of characteristic 7. Let X be a hyperelliptic curve with $g = 6$, so X is defined by $y^2 = f(x)$ where

$$f(x) = \sum_{i=1}^{13} c_i x^i$$

and $c_{13} = 1$. Again we assume that $c_0 = 0$. If we define $f(x)^{(7-1)/2} = \sum_{i=1}^{39} k_i x^i$, then the Cartier-Manin matrix A associated to X is

$$\begin{pmatrix} k_6 & k_5 & k_4 & k_3 & 0 & 0 \\ k_{13} & k_{12} & k_{11} & k_{10} & k_9 & k_8 \\ k_{20} & k_{19} & k_{18} & k_{17} & k_{16} & k_{15} \\ k_{27} & k_{26} & k_{25} & k_{24} & k_{23} & k_{22} \\ k_{34} & k_{33} & k_{32} & k_{31} & k_{30} & k_{29} \\ 0 & 0 & k_{39} & k_{38} & k_{37} & k_{36} \end{pmatrix}$$

With a little bit of information, we can use the determinants of some of the 2×2 minors to determine relationships between the coefficients of $f(x)$. We know $k_3 = c_1^3$, $k_4 = 3c_1^2 c_2$, $k_{39} = 1$, and $k_{38} = 3c_{12}$. Using the minors involving elements from the first two columns with k_{39}, we get that all of the elements in the first two columns must equal zero. Using the minors involving elements from the last two columns with k_3 gives that the last two columns are also all zeros. The last minor that we will need to use is $k_4 \cdot k_{38} - k_3 \cdot k_{39} = 0$. Hence we get a number of equations, but only the following are necessary for determining the form of $f(x)$:

(1) $3c_1^2c_2 \cdot 3c_{12} = c_1^3$

(2) $k_5 = 0 = 3c_1c_2^2 + 3c_1^2c_3$

(3) $k_6 = 0 = c_2^3 + 6c_1c_2c_3 + 3c_1^2c_4$

(4) $k_{37} = 0 = 3c_{12}^2 + 3c_{11}$

(5) $k_{36} = 0 = c_{12}^3 + 6c_{11}c_{12} + 3c_{10}$

(6) $k_{34} = 0 = 3c_{11}^2c_{12} + 3c_{10}c_{12}^2 + 6c_{10}c_{11} + 6c_9c_{12} + 3c_8$

(7) $k_{33} = 0 = c_{11}^3 + 6c_{10}c_{11}c_{12} + 3c_9c_{12}^2 + 3c_{10}^2 + 6c_9c_{11} + 6c_8c_{12} + 3c_7$

(8) $k_{30} = 0 = c_{10}^3 + 6c_9c_{10}c_{11} + 3c_8c_{11}^2 + 3c_9^2c_{12} + 6c_8c_{10}c_{12} + 6c_7c_{11}c_{12} + 3c_6c_{12}^2 + 6c_8c_9 + 6c_7c_{10} + 6c_6c_{11} + 6c_5c_{12} + 3c_4$

(9) $k_{29} = 0 = 3c_9c_{10}^2 + 3c_9^2c_{11} + 6c_8c_{10}c_{11} + 3c_7c_{11}^2 + 6c_8c_9c_{12} + 6c_7c_{10}c_{12} + 6c_6c_{11}c_{12} + 3c_5c_{12}^2 + 3c_8^2 + 6c_7c_9 + 6c_6c_{10} + 6c_5c_{11} + 6c_4c_{12} + 3c_3$

(10) $k_{27} = 0 = c_9^3 + 6c_8c_9c_{10} + 3c_7c_{10}^2 + 3c_8^2c_{11} + 6c_7c_9c_{11} + 6c_6c_{10}c_{11} + 3c_5c_{11}^2 + 6c_7c_8c_{12} + 6c_6c_9c_{12} + 6c_5c_{10}c_{12} + 6c_4c_{11}c_{12} + 3c_3c_{12}^2 + 3c_7^2 + 6c_6c_8 + 6c_5c_9 + 6c_4c_{10} + 6c_3c_{11} + 6c_2c_{12} + 3c_1$

These equations can be simplified to give the following relationships:

(1) $c_1 = 2c_2c_{12}$

(2) $c_2 = c_3c_{12}$

(3) $c_3 = 3c_4c_{12}$

(4) $c_{11} = 6c_{12}^2$

(5) $c_{10} = 4c_{12}^3$

(6) $c_8 = 5c_9c_{12} + 3c_{12}^5$

(7) $c_7 = 5c_9c_{12}^2 + 5c_{12}^6$

(8) $c_4 = c_{12}^9 + 4c_9c_{12}^5 + 4c_9^2c_{12} + c_6c_{12}^2 + 5c_5c_{12}$

(9) $c_5 = 6c_9c_{12}^4 + 6c_9^2 + c_6c_{12}$

(10) $2c_9c_{12}^8 + 4c_9^2c_{12}^4 + 2c_9^3 = 0$

The last equation gives $c_9 = 0$ or $c_9 = 6c_{12}^4$. If $c_9 = 0$, we can solve for c_1, c_2, c_3, c_4, c_5, c_7, c_8, c_9, c_{10}, and c_{11} in terms of c_6 and c_{12}. Then we need to check one more 2×2 minor, the one resulting in $k_{26} = 0$. This gives that

$$\begin{aligned}
k_{26} =& 3c_8c_9^2 + 3c_8^2c_{10} + 6c_7c_9c_{10} + 3c_6c_{10}^2 + 6c_7c_8c_{11} + 6c_6c_9c_{11} + 6c_5c_{10}c_{11} + 3c_4c_{11}^2 + 3c_7^2c_{12} \\
&+ 6c_6c_8c_{12} + 6c_5c_9c_{12} + 6c_4c_{10}c_{12} + 6c_3c_{11}c_{12} + 3c_3c_{12}^2 + 6c_6c_7 + 6c_5c_8 + 6c_4c_9 + 6c_3c_{10} \\
&+ 6c_2c_{11} + 6c_1c_{12} \\
=& c_{12}^{13} = 0.
\end{aligned}$$

If $c_{12} = 0$, $f(x) = x^{13}$ which is not squarefree. This results in X being singular.

If instead $c_9 = 6c_{12}^4$, we can back-substitute variables to get c_1, c_2, c_3, c_4, c_5, c_7, c_8, c_9, c_{10}, and c_{11} in terms of c_6 and c_{12}:

$$[c_1, c_2, c_3, c_4, c_5, c_7, c_8, c_9, c_{10}, c_{11}] = [5c_6c_{12}^5, 6c_6c_{12}^4, 4c_6c_{12}^3, 6c_6c_{12}^2, c_6c_{12}, 0, 5c_{12}^5, 6c_{12}^4, 4c_{12}^3, 6c_{12}^2]$$

This gives $f(x) = x^{13} + c_{12}x^{12} + 6c_{12}^2x^{11} + 4c_{12}^3x^{10} + 6c_{12}^4x^9 + 5c_{12}^5x^8 + c_6x^6 + c_6c_{12}x^5 + 6c_6c_{12}^2x^4 + 4c_6c_{12}^3x^3 + 6c_6c_{12}^4x^2 + 5c_6c_{12}^5x$ which over $\overline{\mathbb{F}}_7$ factors as

$$
\begin{aligned}
f(x) =& x(x^5 + c_{12}x^4 + 6c_{12}^2x^3 + 4c_{12}^3x^2 + 6c_{12}^4x + 5c_{12}^5)(x^7 + c_6) \\
=& x(x - 4c_{12})^5(x + \sqrt[7]{c_6})^7.
\end{aligned}
$$

Thus X is singular, and we see that there are no smooth hyperelliptic curves of genus 6 with $a = 5$ when $p = 7$.

These two examples have a number of similarities, including the algorithm used to determine the form of $f(x)$, the final factored form of $f(x)$, and the fact that $f(x)$ is determined completely by c_g and c_{2g}. The goal, then, is to solidify some of these similarities as truths for any $p > 3$.

3.3.2. Preliminaries. Let X be a hyperelliptic curve defined over a field of characteristic $p > 3$ of genus $g = p - 1$, where X is defined by $y^2 = f(x)$ and $f(x)$ is a degree $2g + 1$ polynomial, $f(x) = \sum_{i=1}^{2g+1} c_i x^i$. We will assume $c_{2g+1} = 1$ so that $f(x)$ is monic, and that $c_1 \neq 0$ so that $f(x)$ does not automatically have repeated roots.

Lemma 3.3.1. *Let $2 \leq i \leq \frac{p-1}{2}$ and $\{m_1, m_2, ..., m_i\}$ be a set of non-negative integers such that $\sum_{\ell=1}^{i} m_\ell = \frac{p-1}{2}$ and $\sum_{\ell=1}^{i} \ell m_\ell = \frac{p-1}{2} + i$. Then*

$$(i-1)m_1 + (i-2)m_2 + ... + 2m_{i-2} + m_{i-1} = (i-1)\left(\frac{p-3}{2}\right) - 1.$$

PROOF. Let $T = (i-1)m_1 + (i-2)m_2 + ... + 2m_{i-2} + m_{i-1}$. Under the assumptions of the statement, we have the following:

$$
\begin{aligned}
T =& i(m_1 + m_2 + ... + m_{i-2} + m_{i-1}) + im_i - im_i - (m_1 + 2m_2 + ... + (i-2)m_{i-2} + (i-1)m_{i-1}) \\
=& i(m_1 + m_2 + ... + m_{i-2} + m_{i-1} + m_i) - (m_1 + 2m_2 + ... + (i-2)m_{i-2} + (i-1)m_{i-1} + im_i) \\
=& i\left(\frac{p-1}{2}\right) - (\frac{p-1}{2} + i) \\
=& (i-1)\left(\frac{p-3}{2}\right) - 1.
\end{aligned}
$$

$\square$

LEMMA 3.3.2. *Let* $2 \leq i \leq \frac{p-1}{2}$ *and* $\{m_{2g-(i-2)}, m_{2g-(i-3)}, ..., m_{2g-1}, m_{2g}, m_{2g+1}\}$ *be a set of non-negative integers such that* $\sum_{\ell=2g-(i-2)}^{2g+1} m_\ell = \frac{p-1}{2}$ *and* $\sum_{\ell=2g-(i-2)}^{2g+1} \ell m_\ell = \left(\frac{p-1}{2}\right)(2g+1) - i$. *Then*

$$(i-1)m_{2g-(i-2)} + (i-2)m_{2g-(i-3)} + ... + 2m_{2g-1} + m_{2g} = i.$$

PROOF. Let $T = (i-1)m_{2g-(i-2)} + (i-2)m_{2g-(i-3)} + ... + 2m_{2g-1} + m_{2g}$. Under the assumptions of the statement, we have the following:

$$
\begin{aligned}
T =& (2g+1)(m_{2g-(i-2)} + m_{2g-(i-3)} + ... + m_{2g-1} + m_{2g} + m_{2g+1}) - \\
& (2g-(i-2))m_{2g-(i-2)} - (2g-(i-3))m_{2g-(i-3)} - ... - (2g-1)m_{2g-1} - 2gm_{2g} - (2g+1)m_{2g+1}
\end{aligned}
$$

$$
\begin{aligned}
=&(2g+1)\left(\frac{p-1}{2}\right)-((2g-(i-2))m_{2g-(i-2)}+(2g-(i-3))m_{2g-(i-3)}+\ldots\\
&+(2g-1)m_{2g-1}+2gm_{2g}+(2g+1)m_{2g+1})\\
=&(2g+1)\left(\frac{p-1}{2}\right)-\left((2g+1)\left(\frac{p-1}{2}\right)-i\right)\\
=&i.
\end{aligned}
$$

$\square$

Lemma 3.3.3. *Let $2 \le i \le \frac{p-1}{2}$ and assume for all j with $1 \le j < i$, $c_j = b_j c_{j+1} c_{2g}$ for some $b_j \in k^*$. Then $k_{\frac{p-1}{2}+i} = c_i^{(p-3)/2} c_{2g}^{(i-1)(p-3)/2-1}\left[\alpha' c_i + \beta c_{i+1} c_{2g}\right]$ for some $\alpha', \beta \in k$.*

Proof. Based on the assumption, we get that for all k with $1 \le k \le i-2$, $c_{i-k} = \prod_{\ell=1}^{k} b_{i-\ell} c_i c_{2g}^k$, since getting c_2 in terms of c_3 and c_{2g} allows us to rewrite c_1 in terms of c_3 and c_{2g}^2, and so on. We can substitute these into the expression for $k_{\frac{p-1}{2}+i}$:

$$
\begin{aligned}
k_{\frac{p-1}{2}+i} =& \sum_{\substack{m_1+m_2+\ldots+m_i=\frac{p-1}{2}\\ m_1+2m_2+\ldots+im_i=\frac{p-1}{2}+i}} \binom{\frac{p-1}{2}}{m_1, m_2, \ldots, m_i} c_1^{m_1} c_2^{m_2} \cdots c_i^{m_i} + \frac{p-1}{2} c_1^{(p-3)/2} c_{i+1}\\
=& \sum \binom{\frac{p-1}{2}}{m_1, m_2, \ldots, m_i} \left(\prod_{\ell=1}^{i-1} b_{i-\ell} c_i c_{2g}^{i-1}\right)^{m_1} \left(\prod_{\ell=1}^{i-2} b_{i-\ell} c_i c_{2g}^{i-2}\right)^{m_2} \ldots (b_{i-1} c_i c_{2g})^{m_{i-1}} c_i^{m_i}\\
&+ \frac{p-1}{2} \left(\prod_{\ell=1}^{i-1} b_{i-\ell} c_i c_{2g}^{i-1}\right)^{(p-3)/2} c_{i+1}\\
=& \sum \left(\alpha c_i^{m_1+m_2+\ldots+m_{i-1}+m_i} c_{2g}^{(i-1)m_1+(i-2)m_2+\ldots+2m_{i-2}+m_{i-1}}\right) + \beta c_i^{(p-3)/2} c_{2g}^{(i-1)(p-3)/2} c_{i+1}\\
=& \sum \left(\alpha c_i^{(p-1)/2} c_{2g}^{(i-1)(p-3)/2-1}\right) + \beta c_i^{(p-3)/2} c_{2g}^{(i-1)(p-3)/2} c_{i+1}
\end{aligned}
$$

$$
\begin{aligned}
&= c_i^{(p-3)/2} c_{2g}^{(i-1)(p-3)/2-1} \left[\sum (\alpha c_i) + \beta c_{i+1} c_{2g} \right] \\
&= c_i^{(p-3)/2} c_{2g}^{(i-1)(p-3)/2-1} \left[\left(\sum \alpha \right) c_i + \beta c_{i+1} c_{2g} \right].
\end{aligned}
$$

If we let $\sum \alpha = \alpha'$, then we have $k_{\frac{p-1}{2}+i} = c_i^{(p-3)/2} c_{2g}^{(i-1)(p-3)/2-1} [\alpha' c_i + \beta c_{i+1} c_{2g}]$. $\square$

For the remainder of this section, let $\sigma = (2g+1)\left(\frac{p-1}{2}\right)$.

LEMMA 3.3.4. *Let* $2 \leq i \leq \frac{p-1}{2}$ *and assume for all* j *with* $1 \leq j \leq i-1$, $c_{2g-j} = b_j c_{2g}^{j+1}$ *for some* $b_j \in k^*$. *Then* $k_{\sigma - i} = \alpha' c_{2g}^i + \frac{p-1}{2} c_{2g-(i-1)}$ *for some* $\alpha' \in k$.

PROOF. Based on the assumption, we can substitute these expressions into $k_{\sigma-i}$ to get the following:

$$
\begin{aligned}
k_{\sigma-i} = & \sum_{\substack{m_{2g-(i-2)}+\ldots+m_{2g+1}=\frac{p-1}{2} \\ \sum s m_s = \sigma - i}} \binom{\frac{p-1}{2}}{m_{2g-(i-2)}, \ldots, m_{2g+1}} c_{2g-(i-2)}^{m_{2g-(i-2)}} c_{2g-(i-3)}^{m_{2g-(i-3)}} \cdots c_{2g+1}^{m_{2g+1}} + \frac{p-1}{2} c_{2g-(i-1)} c_{2g+1}^{(p-3)/2} \\
= & \sum \binom{\frac{p-1}{2}}{m_{2g-(i-2)}, \ldots, m_{2g+1}} \left(b_{i-2} c_{2g}^{i-1}\right)^{m_{2g-(i-2)}} \left(b_{i-2} c_{2g}^{i-2}\right)^{m_{2g-(i-3)}} \cdots \left(b_{i-2} c_{2g}^{i-1}\right)^{m_{2g-(i-2)}} c_{2g}^{m_{2g}} c_{2g+1}^{m_{2g+1}} \\
& + \frac{p-1}{2} c_{2g-(i-1)} c_{2g+1}^{(p-3)/2} \\
= & \sum \binom{\frac{p-1}{2}}{m_{2g-(i-2)}, \ldots, m_{2g+1}} \prod_{\ell=2}^{i-1} b_{i-\ell}^{m_{2g-(i-\ell)}} c_{2g}^{(i-1)m_{2g-(i-2)} + (i-2)m_{2g-(i-2)} + \ldots + 2m_{2g-1} + m_{2g}} \\
& + \frac{p-1}{2} c_{2g-(i-1)} \\
= & \sum \binom{\frac{p-1}{2}}{m_{2g-(i-2)}, \ldots, m_{2g+1}} \prod_{\ell=2}^{i-1} b_{i-\ell}^{m_{2g-(i-\ell)}} c_{2g}^i + \frac{p-1}{2} c_{2g-(i-1)} \\
= & \left(\sum \binom{\frac{p-1}{2}}{m_{2g-(i-2)}, \ldots, m_{2g+1}} \prod_{\ell=2}^{i-1} b_{i-\ell}^{m_{2g-(i-\ell)}} \right) c_{2g}^i + \frac{p-1}{2} c_{2g-(i-1)} \\
= & \alpha' c_{2g}^i + \frac{p-1}{2} c_{2g-(i-1)}.
\end{aligned}
$$

Recall that $c_{2g+1} = 1$ and that is why it dropped out of the expression. Therefore, $k_{\sigma-i} = \alpha' c_{2g}^i + \frac{p-1}{2} c_{2g-(i-1)}$ for some $\alpha' \in k$. $\square$

Lemma 3.3.5. *Let $2 \le i \le \frac{p-1}{2}$ and assume for all j with $1 \le j < i$, $c_j = b_j c_{j+1} c_{2g}$ for some $b_j \in k^*$ and $k_{\frac{p-1}{2}+i} = 0$. Then $c_i = b_i c_{i+1} c_{2g}$ with $b_i \in k$.*

Proof. Based on the assumptions, lemma 3.3.3 applies and we see that

$$k_{\frac{p-1}{2}+i} = 0 = c_i^{(p-3)/2} c_{2g}^{(i-1)(p-3)/2-1} \left[\alpha' c_i + \beta c_{i+1} c_{2g}\right].$$

Since $c_1 \neq 0$ and under the assumptions $c_1 = \prod_{\ell=1}^{i-1} b_{i-\ell} c_i c_{2g}^{i-1}$, we must have $c_i \neq 0$ and $c_{2g} \neq 0$ as well. Hence we get that $c_i = -(\alpha')^{-1} \beta c_{i+1} c_{2g}$. $\square$

Lemma 3.3.6. *Let $2 \le i \le \frac{p-1}{2}$ and assume for all j with $1 \le j \le i-1$, $c_{2g-j} = b_j c_{2g}^{j+1}$ for some $b_j \in k^*$ and $k_{\sigma-i} = 0$. Then $c_{2g-(i-1)} = b_{i-1} c_{2g}^{i}$ with $b_i \in k$.*

Proof. Under these assumptions, lemma 3.3.4 applies and

$$k_{\sigma-i} = 0 = \alpha' c_{2g}^{i} + \frac{p-1}{2} c_{2g-(i-1)}.$$

Hence, $c_{2g-(i-1)} = -\alpha' \left(\frac{p-1}{2}\right)^{-1} c_{2g}^{i}$. $\square$

Lemma 3.3.7. *Let $\frac{p+3}{2} \le i \le p-1$ and assume for all j with $\frac{p+3}{2} \le j < i$ that $c_{2g-(j-1)} \in k[c_{2g-g/2}, c_{2g}]$, $k_{\sigma-i} = 0$, and the assumptions of lemma 3.3.6 are satisfied. Then $c_{2g-(i-1)} \in k[c_{2g-g/2}, c_{2g}]$.*

Proof. If $k_{\sigma-i} = 0$, then

$$0 = \sum_{\substack{m_{2g-(i-2)}+\ldots+m_{2g+1}=\frac{p-1}{2} \\ \sum s m_s = \sigma - i}} \binom{\frac{p-1}{2}}{m_{2g-(i-2)}, \ldots, m_{2g+1}} c_{2g-(i-2)}^{m_{2g-(i-2)}} c_{2g-(i-3)}^{m_{2g-(i-3)}} \cdots c_{2g+1}^{m_{2g+1}} + \frac{p-1}{2} c_{2g-(i-1)} c_{2g+1}^{(p-3)/2}.$$

If we consider the coefficients present within this sum, we have $c_{2g-(i-d-1)}$ for $1 \leq d \leq i$, and once $i-d \leq \frac{p-1}{2}$, then we know $c_{2g-(i-d-1)} = b_{i-d-1}c_{2g}^{i-d}$, using the conclusion of lemma 3.3.6. When $i-d = \frac{p-1}{2}+1$, $c_{2g-(i-d-1)} = c_{2g-g/2}$. Let $c_{2g-(j-1)} = p_j(c_{2g-g/2}, c_{2g})$, a polynomial in $c_{2g-g/2}$ and c_{2g}, with the conditions on j as assumed in the lemma statement. Then

$$0 = \sum \binom{\frac{p-1}{2}}{m_{2g-(i-2)}, \ldots, m_{2g+1}} (p_{i-1})^{m_{2g-(i-2)}} (p_{i-2})^{m_{2g-(i-3)}} \cdots (p_{g/2+1})^{m_{2g-(g/2+1)}} c_{2g-g/2}^{m_{2g-g/2}}$$
$$\cdot (b_{g/2-1}c_{2g}^{g/2})^{m_{2g-(g/2-1)}} \cdots (b_2 c_{2g}^3)^{m_{2g-2}} (b_1 c_{2g}^2)^{m_{2g-1}} c_{2g}^{m_{2g}} + \frac{p-1}{2} c_{2g-(i-1)}.$$

We see that the resulting terms in the sum are still polynomials of $c_{2g-g/2}$ and c_{2g}, so we can call the sum $p(c_{2g-g/2}, c_{2g})$. Now,

$$0 = p(c_{2g-g/2}, c_{2g}) + \frac{p-1}{2} c_{2g-(i-1)},$$

and we get that $c_{2g-(i-1)} = -\left(\frac{p-1}{2}\right)^{-1} p(c_{2g-g/2}, c_{2g})$. Thus, $c_{2g-(i-1)} \in k[c_{2g-g/2}, c_{2g}]$. □

Lemma 3.3.8. *Let $p+2 \leq i \leq \frac{3p-3}{2}$ and assume for all j with $p+2 \leq j < i$ that $c_{2g-(j-1)} \in k[c_{g-1}, c_g, c_{2g-g/2}, c_{2g}]$, $k_{\sigma-i} = 0$, and the assumptions of lemmas 3.3.6 and 3.3.7 are satisfied. Then $c_{2g-(i-1)} \in k[c_{g-1}, c_g, c_{2g-g/2}, c_{2g}]$.*

Proof. As in the previous lemma, the expression for $k_{\sigma-i}$ contains $c_{2g-(i-d-1)}$ for $1 \leq d \leq i$, and once $\frac{p+3}{2} \leq i-d \leq p-1$, $c_{2g-(i-d-1)} \in k[c_{2g-g/2}, c_{2g}]$ by lemma 3.3.7. Let these be represented by polynomials $p_{i-d}(c_{2g-g/2}, c_{2g})$. Once $i-d \leq \frac{p-1}{2}$, then we know $c_{2g-(i-d-1)} = b_{i-d-1}c_{2g}^{i-d}$, using the conclusion of lemma 3.3.6. When $i-d = \frac{p-1}{2}+1$, $c_{2g-(i-d-1)} = c_{2g-g/2}$, when $i-d = p$, $c_{2g-(i-d-1)} = c_g$, and when $i-d = p+1$, $c_{2g-(i-d-1)} = c_{g-1}$. Let $c_{2g-(j-1)} = q_j(c_{g-1}, c_g, c_{2g-g/2}, c_{2g})$, a polynomial in $c_{g-1}, c_g, c_{2g-g/2}$, and c_{2g}, with the conditions on j as assumed in the lemma statement. Since we are assuming $k_{\sigma-i} = 0$, we get

$$0 = \sum_{\substack{m_{2g-(i-2)}+\ldots+m_{2g+1}=\frac{p-1}{2} \\ \sum sm_s=\sigma-i}} \binom{\frac{p-1}{2}}{m_{2g-(i-2)}, \ldots, m_{2g+1}} (q_{i-1})^{m_{2g-(i-2)}} (q_{i-2})^{m_{2g-(i-3)}} \cdots (q_{g+3})^{m_{2g-(g+2)}}$$

$$\cdot c_{g-1}^{m_{g-1}} c_g^{m_g} (p_g)^{m_{2g-(g-1)}} \cdots (p_{g/2+2})^{m_{2g-(g/2+1)}} (b_{g/2-1} c_{2g}^{g/2})^{m_{2g-(g/2-1)}} \cdots (b_1 c_{2g}^2)^{m_{2g-1}} c_{2g}^{m_{2g}} + \frac{p-1}{2} c_{2g-(i-1)}.$$

Each term in the sum is a product of polynomials in $c_{g-1}, c_g, c_{2g-g/2}$ and c_{2g}, so we can call the sum $q(c_{g-1}, c_g, c_{2g-g/2}, c_{2g})$. This gives

$$0 = q(c_{g-1}, c_g, c_{2g-g/2}, c_{2g}) + \frac{p-1}{2} c_{2g-(i-1)},$$

which means $c_{2g-(i-1)} = -\left(\frac{p-1}{2}\right)^{-1} q(c_{g-1}, c_g, c_{2g-g/2}, c_{2g})$. Therefore, $c_{2g-(i-1)} \in k[c_{g-1}, c_g, c_{2g-g/2}, c_{2g}]$.

$\square$

3.3.3. The Main Result.

Theorem 3.3.9. *Let X be a hyperelliptic curve defined over a field of characteristic $p > 3$ of genus $g = p - 1$, where X is defined above. If X has $a = g - 1$, then $f(x) \in k[x, c_g, c_{2g-g/2}, c_{2g}]$.*

Proof. As in Sections 3.1 and 3.2, we will use the Cartier-Manin matrix A to determine any restrictions on the coefficients of $f(x)$. In this case, there will again be $g - \frac{p+1}{2} = \frac{p-3}{2}$ zeros in A_1 and A_g, meaning A is of the following form, where $\sigma = (2g+1)\left(\frac{p-1}{2}\right) = \frac{2p^2-3p+1}{2}$:

$$\begin{pmatrix} k_{\frac{p-1}{2}+\frac{p-1}{2}} & k_{\frac{p-1}{2}+\frac{p-3}{2}} & \dots & k_{\frac{p-1}{2}+2} & k_{\frac{p-1}{2}+1} & c_1^{(p-1)/2} & 0 & \dots & 0 & 0 \\ \vdots & \ddots & & \vdots & \vdots & k_{\frac{p-1}{2}+p} & k_{\frac{p-1}{2}+(p-1)} & \dots & k_{\frac{p-1}{2}+\frac{p+5}{2}} & k_{\frac{p-1}{2}+\frac{p+3}{2}} \\ \vdots & & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ k_{\sigma-\frac{p+3}{2}} & k_{\sigma-\frac{p+5}{2}} & \dots & k_{\sigma-(p-1)} & k_{\sigma-p} & k_{\sigma-(p+1)} & k_{\sigma-(p+2)} & \dots & k_{\sigma-\frac{3p-3}{2}} & k_{\sigma-\frac{3p-1}{2}} \\ 0 & 0 & \dots & 0 & 1 & k_{\sigma-1} & k_{\sigma-2} & \dots & k_{\sigma-\frac{p-3}{2}} & k_{\sigma-\frac{p-1}{2}} \end{pmatrix}$$

First, we see

$$c_1^{(p-1)/2} \cdot 1 - k_{\frac{p-1}{2}+1} \cdot k_{\sigma-1} = 0.$$

Since $k_{\frac{p-1}{2}+1} = \frac{p-1}{2} c_2 c_1^{(p-3)/2}$ and $k_{\sigma-1} = \frac{p-1}{2} c_{2g}$,

$$\begin{aligned} 0 &= c_1^{(p-1)/2} \cdot 1 - \frac{p-1}{2} c_2 c_1^{(p-3)/2} \cdot \frac{p-1}{2} c_{2g} \\ &= c_1^{(p-3)/2} \left(c_1 - \left(\frac{p-1}{2} \right)^2 c_2 c_{2g} \right). \end{aligned}$$

Since we are assuming $c_1 \neq 0$ so that $f(x)$ is squarefree, we must have

$$c_1 = \left(\frac{p-1}{2} \right)^2 c_2 c_{2g}.$$

Note that this means $c_2 \neq 0$ and $c_{2g} \neq 0$.

Next, we will consider what information we can get from A_1. For $2 \leq i \leq \frac{p-1}{2}$,

$$k_{\frac{p-1}{2}+i} \cdot 1 - 0 \cdot k_{\frac{p-1}{2}+1} = 0,$$

so $k_{\frac{p-1}{2}+i} = 0$. When $i = 2$,

$$\begin{aligned} k_{\frac{p-1}{2}+2} =& \frac{p-1}{2}\left(c_1^{(p-5)/2}c_2^2 + c_1^{(p-3)/2}c_3\right) = 0 \\ =& \frac{p-1}{2}\left[\left(\left(\frac{p-1}{2}\right)^2 c_2c_{2g}\right)^{(p-5)/2} c_2^2 + \left(\left(\frac{p-1}{2}\right)^2 c_2c_{2g}\right)^{(p-3)/2} c_3\right] = 0 \\ =& \left(\frac{p-1}{2}\right)^{(p-4)} c_2^{(p-3)/2}c_{2g}^{(p-5)/2}\left[c_2 + \left(\frac{p-1}{2}\right)^2 c_{2g}c_3\right] = 0 \end{aligned}$$

We know $c_2 \neq 0$ and $c_{2g} \neq 0$, so

$$c_2 = -\left(\frac{p-1}{2}\right)^2 c_3c_{2g}.$$

Now, when we consider $i = 3$, lemma 3.3.5 applies to give c_3 in terms of c_4 and c_{2g}. Repeatedly applying lemma 3.3.5 gives $c_{i-k} = \gamma_{i-k}c_{i+1}c_{2g}^{k+1}$ for $0 \leq k \leq i-2$, which means we have c_m in terms of $c_{g/2+1}$ and c_{2g} for $1 \leq m \leq \frac{g}{2}$.

Let us next consider what information we can learn about the coefficients of $f(x)$ from A_g. For $2 \leq i \leq \frac{p-1}{2}$,

$$k_{\sigma-i} \cdot c_1^{(p-1)/2} - k_{\sigma-1} \cdot 0 = 0$$

and since $c_1 \neq 0$, we have $k_{\sigma-i} = 0$. Consider first when $i = 2$.

$$\begin{aligned} k_{\sigma-2} &= \left(\frac{p-1}{2}\right) c_{2g-1}c_{2g+1}^{(p-3)/2} + \left(\frac{p-1}{2}\right)\left(\frac{p-3}{2}\right) c_{2g}^2c_{2g+1}^{(p-5)/2}\frac{1}{2} = 0 \\ &= \left(\frac{p-1}{2}\right)\left[c_{2g-1} + \frac{1}{2}\left(\frac{p-3}{2}\right)c_{2g}^2\right] = 0. \end{aligned}$$

This gives $c_{2g-1} = -2^{-1}\left(\frac{p-3}{2}\right)c_{2g}^2$. Now lemma 3.3.6 applies to give $c_{2g-2} = b_2 c_{2g}^3$, and repeatedly applying this lemma allows us to solve for coefficients of $f(x)$ in terms of the last coefficient c_{2g}. We now have $c_{2g-g/2+1}, ..., c_{2g-2}, c_{2g-1}$ in terms of c_{2g}.

Next we move up to A_{g-1} for more information. For $\frac{p+3}{2} \leq i \leq p-1$,

$$k_{\sigma-i} \cdot 1 - k_{\sigma-p} \cdot 0 = 0$$

which forces $k_{\sigma-i} = 0$. Consider first when $i = \frac{p+3}{2} = \frac{g}{2} + 2$. Then

$$0 = \sum_{\substack{m_{2g-g/2}+...+m_{2g+1}=\frac{p-1}{2} \\ \sum sm_s=\sigma-(p+3)/2}} \binom{\frac{p-1}{2}}{m_{2g-g/2}, \ldots, m_{2g+1}} c_{2g-g/2}^{m_{2g-g/2}} c_{2g-g/2+1}^{m_{2g-g/2+1}} \cdots c_{2g+1}^{m_{2g+1}} + \frac{p-1}{2} c_{2g-g/2-1} c_{2g+1}^{(p-3)/2}.$$

We just found that $c_{2g-1}, c_{2g-2}, ..., c_{2g-g/2+1}$ can be written in terms of c_{2g}, so this expression becomes

$$0 = \sum_{\substack{m_{2g-g/2}+...+m_{2g+1}=\frac{p-1}{2} \\ \sum sm_s=\sigma-i}} \beta c_{2g-g/2}^{m_{2g-g/2}} (c_{2g}^{g/2})^{m_{2g-g/2+1}} \cdots (c_{2g}^2)^{m_{2g+1}} c_{2g}^{m_{2g}} c_{2g+1}^{m_{2g+1}} + \frac{p-1}{2} c_{2g-g/2-1} c_{2g+1}^{(p-3)/2},$$

where β is the product of the binomial coefficient with the coefficients $b_j^{m_{2g-j}}$ for $1 \leq j \leq \frac{p-1}{2}$. Since $c_{2g+1} = 1$,

$$0 = \sum \beta c_{2g-g/2}^{m_{2g-g/2}} c_{2g}^{g/2(m_{2g-g/2+1})+(g/2+1)(m_{2g-g/2+2})+...+2m_{2g-1}+m_{2g}} + \frac{p-1}{2} c_{2g-g/2-1},$$

which means

$$c_{2g-g/2-1} = -\left(\frac{p-1}{2}\right)^{-1} \left[\sum \beta c_{2g-g/2}^{m_{2g-g/2}} c_{2g}^{g/2(m_{2g-g/2+1})+(g/2+1)(m_{2g-g/2+2})+...+2m_{2g-1}+m_{2g}}\right].$$

Thus we see that $c_{2g-g/2-1} \in k[c_{2g-g/2}, c_{2g}]$. When we consider $i = \frac{p+5}{2}$, lemma 3.3.7 applies to give $c_{2g-g/2-2} \in k[c_{2g-g/2}, c_{2g}]$, and repeatedly applying lemma 3.3.7 gives $c_{g+1}, c_{g+2}, ...c_{2g-g/2-3} \in k[c_{2g-g/2}, c_{2g}]$.

Now let $p+2 \le i \le \frac{3p-3}{2}$. We have

$$k_{\sigma-i} \cdot k_{\frac{p-1}{2}} - k_{\sigma-(p-1)} \cdot 0 = 0$$

and since $c_1 \neq 0$, we must have $k_{\sigma-i} = 0$. When $i = p+2$,

$$\begin{aligned}
0 &= \sum_{\substack{m_{2g-p}+\ldots+m_{2g+1}=\frac{p-1}{2} \\ \sum s m_s = \sigma-(p+2)}} \binom{\frac{p-1}{2}}{m_{2g-p}, \ldots, m_{2g+1}} c_{2g-p}^{m_{2g-p}} c_{2g-(p-1)}^{m_{2g-(p-1)}} \cdots c_{2g}^{m_{2g}} c_{2g+1}^{m_{2g+1}} + \frac{p-1}{2} c_{2g-(p+1)} c_{2g+1}^{(p-3)/2} \\
&= \sum \binom{\frac{p-1}{2}}{m_{2g-(g+1)}, \ldots, m_{2g+1}} c_{2g-(g+1)}^{m_{2g-(g+1)}} c_{2g-g}^{m_{2g-g}} \cdots c_{2g}^{m_{2g}} c_{2g+1}^{m_{2g+1}} + \frac{p-1}{2} c_{2g-(p+1)} c_{2g+1}^{(p-3)/2} \\
&= \sum \binom{\frac{p-1}{2}}{m_{g-1}, \ldots, m_{2g+1}} c_{g-1}^{m_{g-1}} c_{g}^{m_{g}} \cdots c_{2g}^{m_{2g}} c_{2g+1}^{m_{2g+1}} + \frac{p-1}{2} c_{g-2} c_{2g+1}^{(p-3)/2}.
\end{aligned}$$

Since $c_{2g+1} = 1$, we can solve for c_{g-2}:

$$c_{g-2} = -\left(\frac{p-1}{2}\right)^{-1} \left(\sum \binom{\frac{p-1}{2}}{m_{g-1}, \ldots, m_{2g+1}} c_{g-1}^{m_{g-1}} c_{g}^{m_{g}} \cdots c_{2g}^{m_{2g}} \right).$$

We have $c_{g+1}, c_{g+2}, ...c_{2g-g/2-2}, c_{2g-g/2-1} \in k[c_{2g-g/2}, c_{2g}]$, and we know from above that $c_{2g-g/2+1}, ..., c_{2g-2}, c_{2g-1} \in k[c_{2g}]$. Hence, $c_{g-2} \in k[c_{g-1}, c_g, c_{2g-g/2}, c_{2g}]$.

When $i = p+3$, lemma 3.3.8 applies to show that $c_{g-3} \in k[c_{g-1}, c_g, c_{2g-g/2}, c_{2g}]$. Repeatedly applying lemma 3.3.8 gives $c_{g/2+1}, c_{g/2+2}, ..., c_{g-4} \in k[c_{g-1}, c_g, c_{2g-g/2}, c_{2g}]$ as well.

Let us momentarily recap what we have solved for thus far. We have $c_1, c_2, ...c_{g/2} \in k[c_{g/2+1}, c_{2g}]$, $c_{g/2+1}, c_{g/2+2}, ..., c_{g-3}, c_{g-2} \in k[c_{g-1}, c_g, c_{2g-g/2}, c_{2g}]$, $c_{g+1}, c_{g+2}, ...c_{2g-g/2-2}, c_{2g-g/2-1} \in k[c_{2g-g/2}, c_{2g}]$, and $c_{2g-g/2+1}, ..., c_{2g-2}, c_{2g-1} \in k[c_{2g}]$. Overall, we have found $c_i \in k[c_{g-1}, c_g, c_{2g-g/2}, c_{2g}]$ for $1 \leq i \leq 2g-1$ and $i \neq g-1, g, 2g-g/2$.

The last step in finishing the proof is to show that $c_{g-1} \in k[c_g, c_{2g-g/2}, c_{2g}]$. So consider the following 2×2 minor:

$$k_{\sigma-p} \cdot k_{\sigma-1} - 1 \cdot k_{\sigma-(p+1)} = 0.$$

We know

$$k_{\sigma-p} = \sum_{\substack{m_{g+1}+...+m_{2g+1}=\frac{p-1}{2} \\ \sum sm_s=\sigma-p}} \binom{\frac{p-1}{2}}{m_{g+1}, \ldots, m_{2g+1}} c_{g+1}^{m_{g+1}} c_{g+2}^{m_{g+2}} \cdots c_{2g+1}^{m_{2g+1}} + \frac{p-1}{2} c_g c_{2g+1}^{(p-3)/2}.$$

We also know $k_{\sigma-1} = \dfrac{p-1}{2} c_{2g}$, and

$$k_{\sigma-(p+1)} = \sum_{\substack{m_g+...+m_{2g+1}=\frac{p-1}{2} \\ \sum sm_s=\sigma-(p+1)}} \binom{\frac{p-1}{2}}{m_g, \ldots, m_{2g+1}} c_g^{m_g} c_{g+1}^{m_{g+1}} \cdots c_{2g+1}^{m_{2g+1}} + \frac{p-1}{2} c_{g-1} c_{2g+1}^{(p-3)/2}.$$

Hence we have the following equality:

$$\begin{aligned} 0 =& \frac{p-1}{2} c_{2g} \left(\sum \binom{\frac{p-1}{2}}{m_{g+1}, \ldots, m_{2g+1}} c_{g+1}^{m_{g+1}} c_{g+2}^{m_{g+2}} \cdots c_{2g+1}^{m_{2g+1}} \right) + \frac{p-1}{2} c_{2g} \frac{p-1}{2} c_g c_{2g+1}^{(p-3)/2} \\ & - \sum \binom{\frac{p-1}{2}}{m_g, \ldots, m_{2g+1}} c_g^{m_g} c_{g+1}^{m_{g+1}} \cdots c_{2g+1}^{m_{2g+1}} - \frac{p-1}{2} c_{g-1} c_{2g+1}^{(p-3)/2}. \end{aligned}$$

This allows us to solve for c_{g-1}, and using the fact that $c_{2g+1} = 1$ gives

$$c_{g-1} = \left(\frac{p-1}{2}\right)^{-1} \left[\frac{p-1}{2} c_{2g} \left(\sum \binom{\frac{p-1}{2}}{m_{g+1}, \ldots, m_{2g+1}} c_{g+1}^{m_{g+1}} c_{g+2}^{m_{g+2}} \cdots c_{2g}^{m_{2g}}\right) + \left(\frac{p-1}{2}\right)^2 c_g c_{2g}\right.$$
$$\left. - \sum \binom{\frac{p-1}{2}}{m_g, \ldots, m_{2g+1}} c_g^{m_g} c_{g+1}^{m_{g+1}} \cdots c_{2g}^{m_{2g}}\right].$$

Note that the expression on the right includes only c_i for $g \leq i \leq 2g$. Since we have found $c_j \in k[c_{2g-g/2}, c_{2g}]$ for $g+1 \leq j \leq 2g-1$ and $j \neq 2g - g/2$, we see that this expression gives $c_{g-1} \in k[c_g, c_{2g-g/2}, c_{2g}]$.

Therefore, we have found $c_i \in k[c_g, c_{2g-g/2}, c_{2g}]$ for $1 \leq i \leq 2g-1$ and $i \neq g, 2g-g/2, 2g$. This gives the desired result that $f(x) \in k[x, c_g, c_{2g-g/2}, c_{2g}]$. $\square$

CHAPTER 4

Computations and Examples for Small Primes

4.1. For $p = 3$

We see from Elkin's bound that hyperelliptic curves defined over $\overline{\mathbb{F}}_3$ with $a = g - 1$ will only occur when $g < 5$. By the results in Chapter 3, in fact such a curve will only occur for $g < 3$. In fact, genus 3 hyperelliptic curves have been studied extensively, and it was previously known that curves with $a = 2$ do not exist [EP07]. It is also known that genus 2 hyperelliptic curves with $a = 1$ exist for all $p \geq 3$. Hence for $p = 3$, genus 2 hyperelliptic curves are the only hyperelliptic curves with $a = g - 1$.

4.2. For $p = 5$

According to Elkin's bound, hyperelliptic curves with $a = g - 1$ will only occur when $g < \frac{15}{2}$. For $p = 5$ it is known that such hyperelliptic curves exist with genus 2 and with genus 3 [EP07]. When $g = 3$, they in fact occur with both p-rank 0 and 1.

Remark. Due to genus 3 curves with $a = 2$ occurring with both p-rank 0 and 1, there are still three possibilities for their Ekedahl-Oort type. This topic is discussed further in Chapter 5.

Example 4.2.1. We see in Figure 4.1 that over the base field $\mathbb{F}_5$ there are almost an equal amount of curves with p-rank 0 and p-rank 1. This is surprising because it is expected that curves having $a = 2$ with p-rank 1 will form a subspace of dimension 2 in the dimension 5 space of smooth genus 3 hyperelliptic curves, and the curves having $a = 2$ with p-rank 0

FIGURE 4.1. Hyperelliptic curves and their p-rank in characteristic 5 with $g = 3$ and $a = 2$.

```
F=GF(5)
R.<x>=PolynomialRing(F)
N=0
V=VectorSpace(F, 6)
for m in V:
    f=m[0]*x+m[1]*x^2+m[2]*x^3+m[3]*x^4+m[4]*x^5+m[5]*x^6+x^7
    if f.is_squarefree()==True:
        C=HyperellipticCurve(f)
        B=C.Cartier_matrix()
        if B.determinant()==0:
            if B.rank()==1:
                N=N+1;
                [f,C.p_rank()]
N
[x^7 + x^5 + x^3 + 4*x, 0]
[x^7 + x^5 + 3*x^3 + 2*x, 1]
[x^7 + x^5 + 4*x^3 + x, 0]
[x^7 + 2*x^5 + x^3 + 3*x, 0]
[x^7 + 2*x^5 + 2*x^3 + x, 1]
[x^7 + 2*x^5 + 4*x^3 + 2*x, 0]
[x^7 + 3*x^5 + x^3 + 2*x, 0]
[x^7 + 3*x^5 + 2*x^3 + 4*x, 1]
[x^7 + 3*x^5 + 4*x^3 + 3*x, 0]
[x^7 + 4*x^5 + x^3 + x, 0]
[x^7 + 4*x^5 + 3*x^3 + 3*x, 1]
[x^7 + 4*x^5 + 4*x^3 + 4*x, 0]
[x^7 + x^6 + x^5 + 2*x^3 + x^2 + 3*x, 1]
[x^7 + x^6 + x^5 + 3*x^3 + 4*x^2 + 2*x, 1]
[x^7 + x^6 + 3*x^5 + x^3 + 4*x^2 + 3*x, 1]
[x^7 + x^6 + 3*x^5 + 2*x^3 + 3*x^2 + x, 0]
[x^7 + x^6 + 3*x^5 + 3*x^3 + 2*x^2 + 4*x, 0]
[x^7 + x^6 + 3*x^5 + 4*x^3 + x^2 + 2*x, 1]
[x^7 + 2*x^6 + 2*x^5 + x^3 + 3*x^2 + 2*x, 1]
[x^7 + 2*x^6 + 2*x^5 + 2*x^3 + x^2 + 4*x, 0]
[x^7 + 2*x^6 + 2*x^5 + 3*x^3 + 4*x^2 + x, 0]
[x^7 + 2*x^6 + 2*x^5 + 4*x^3 + 2*x^2 + 3*x, 1]
[x^7 + 2*x^6 + 4*x^5 + 2*x^3 + 2*x^2 + 2*x, 1]
[x^7 + 2*x^6 + 4*x^5 + 3*x^3 + 3*x^2 + 3*x, 1]
[x^7 + 3*x^6 + 2*x^5 + x^3 + 2*x^2 + 2*x, 1]
[x^7 + 3*x^6 + 2*x^5 + 2*x^3 + 4*x^2 + 4*x, 0]
[x^7 + 3*x^6 + 2*x^5 + 3*x^3 + x^2 + x, 0]
[x^7 + 3*x^6 + 2*x^5 + 4*x^3 + 3*x^2 + 3*x, 1]
[x^7 + 3*x^6 + 4*x^5 + 2*x^3 + 3*x^2 + 2*x, 1]
[x^7 + 3*x^6 + 4*x^5 + 3*x^3 + 2*x^2 + 3*x, 1]
[x^7 + 4*x^6 + x^5 + 2*x^3 + 4*x^2 + 3*x, 1]
[x^7 + 4*x^6 + x^5 + 3*x^3 + x^2 + 2*x, 1]
[x^7 + 4*x^6 + 3*x^5 + x^3 + x^2 + 3*x, 1]
[x^7 + 4*x^6 + 3*x^5 + 2*x^3 + 2*x^2 + x, 0]
[x^7 + 4*x^6 + 3*x^5 + 3*x^3 + 3*x^2 + 4*x, 0]
[x^7 + 4*x^6 + 3*x^5 + 4*x^3 + 4*x^2 + 2*x, 1]
36
```

will form a subspace of dimension 1. Hence, we should expect to see far fewer of these curves with p-rank 0.

It is next worth investigating $g = 4, 5, 6$, and 7, but Theorems 3.1.1 and 3.2.3 in Chapter 3 show that for $g = 5, 6$ and 7, there are no smooth hyperelliptic curves of such a genus with $a = g - 1$. As we saw in Example 3.3.1, there are no smooth hyperelliptic curves of $g = 4$ with $a = 3$ defined over a field of characteristic 5. Hence, the case $p = 5$ is completely determined, with curves having $a = g - 1$ only existing when $g = 2$ and $g = 3$.

4.3. For $p = 7$

Elkin's bound for $p = 7$ gives that for a hyperelliptic curve with $a = g - 1$, we must have $g < \frac{21}{2}$, so we are interested in looking for curves with genus up to 10. Theorems 3.1.1 and 3.2.3 show that such a curve will not exist with $g \geq p$, so in fact we only need to study $g = 2, 3, 4, 5$ and 6. It was previously shown that genus 2 curves exist with $a = 1$ in characteristic 7.

Example 4.3.1. Hyperelliptic curves of genus 3 with $a = 2$ exist, and as occurred for $p = 5$, they exist with p-rank 0 and 1, meaning there are three possibilities for their Ekedahl-Oort type. In this case, as expected, there are far more such curves with p-rank 1 than p-rank 0 over the base field $\mathbb{F}_7$.

It is still open whether or not curves of genus 4 exist with $a = 3$. It is shown in Figure 4.2 that these curves do not exist over $\mathbb{F}_7$, but they could still exist over some field extension. There are 49^9 possible curves branched at ∞ over the first field extension, $\mathbb{F}_{49}$. Rather than searching all of these curves, we can fix additional branch points at $x = 0$ and 1 and this brings the possible number of curves down to 49^7. This is still too many curves to check computationally in any reasonable amount of time, but it is possible to check a large number of random curves for $a = 3$. After checking $1,000,000$ curves of this form, none were found

FIGURE 4.2. Computations in Sage show there are no genus 4 curves with $a = 3$ over $\mathbb{F}_7$ and that a random check of 1,000,000 curves over $\mathbb{F}_{49}$ did not find any genus 4 curves with $a = 3$.

```
F=GF(7)
R.<x>=PolynomialRing(F)
N=0
V=VectorSpace(F, 8)
for m in V:
    f=m[1]*x+m[2]*x^2+m[3]*x^3+m[4]*x^4+m[5]*x^5+m[6]*x^6+m[7]*x^7+m[0]*x\
      ^8+x^9
    if f.is_squarefree()==True:
        C=HyperellipticCurve(f)
        B=C.Cartier_matrix()
        if B.determinant()==0:
            if B.rank()==1:
                N=N+1;
                C
N
0
```

```
F=GF(49,'a')
R.<x>=PolynomialRing(F)
N=0
for i in range(1000000):
    m=random_vector(F,7)
    f=(x-1)*(m[0]*x+m[1]*x^2+m[2]*x^3+m[3]*x^4+m[4]*x^5+m[5]*x^6+m[6]*x\
      ^7+x^8)
    if f.is_squarefree()==True:
        C=HyperellipticCurve(f)
        B=C.Cartier_matrix()
        if B.determinant()==0:
            if B.rank()==1:
                N=N+1;
                C
N
0
```

to have $a = 3$. This can be seen in Figure 4.2. However, this is a very small portion of the total number of curves, so it is possible that such a curve does still exist. Furthermore, not finding any over $\mathbb{F}_{49}$ does not mean such a curve doesn't still exist over a larger extension, although it does mean that the occurrence is not very likely.

When $g = 5$, we see similar results. It is still open whether or not curves of genus 5 exist with $a = 4$. Figure 4.3 shows that when restrictions are placed on the coefficients of $f(x)$, for $y^2 = f(x)$, to force the Cartier-Manin matrix to have rank one, there are no genus 5 curves over $\mathbb{F}_7$ with $a = 4$.

FIGURE 4.3. Computations in Sage show there are no genus 5 curves with $a = 4$ over $\mathbb{F}_7$.

```
F=GF(7)
R.<x>=F[]
N=0
V=VectorSpace(F, 7)
for m in V:
    c2=m[0]
    c3=m[1]
    c4=m[2]
    c6=m[3]
    c7=m[4]
    c8=2*m[6]^3+5*m[5]*m[6]
    c9=m[5]
    c10=m[6]
    c5=2*c9^3+5*c8*c9*c10+6*c7*c10^2+6*c8^2+5*c7*c9+5*c6*c10
    c1=6*c7*c8^2+6*c7^2*c9+5*c6*c8*c9+6*c5*c9^2+5*c6*c7*c10+5*c5*c8*c10\
       +5*c4*c9*c10+6*c3*c10^2+6*c6^2+5*c5*c7+5*c4*c8+5*c3*c9+5*c2*c10
    if c2^3+6*c1*c2*c3+3*c1^2*c4==0:
        if c9^3+6*c8*c9*c10+3*c7*c10^2+3*c8^2+6*c7*c9+6*c6*c10+3*c5==0:
            if c3^3+6*c2*c3*c4+3*c1*c4^2+3*c2^2*c5+6*c1*c3*c5+6*c1*c2*c6\
               +3*c1^2*c7==0:
                if 3*c4^2*c5+3*c3*c5^2+6*c3*c4*c6+6*c2*c5*c6+3*c1*c6^2+3*\
                   c3^2*c7+6*c2*c4*c7+6*c1*c5*c7+6*c2*c3*c8+6*c1*c4*c8+3*\
                   c2^2*c9+6*c1*c3*c9+6*c1*c2*c10+3*c1^2==0:
                    f=x^11+c10*x^10+c9*x^9+c8*x^8+c7*x^7+c6*x^6+c5*x^5+c4\
                      *x^4+c3*x^3+c2*x^2+c1*x
                    if f.is_squarefree()==True:
                        C=HyperellipticCurve(f)
                        B=C.Cartier_matrix()
                        if B.determinant()==0:
                            if B.rank()==1:
                                N=N+1;
                                [f,C.p_rank()]
N
0
```

There are 49^{11} possible curves branched at ∞ over the first field extension, $\mathbb{F}_{49}$. Rather than searching all of these curves, we can fix an additional branch point at $x = 0$, and then use information from the Cartier-Manin matrix, again forcing the matrix to have rank one, to further shrink the search space. At this point, it was possible to check a large number of random curves to see if the had $a = 4$, as shown in Figure 4.4. After checking 21,000,000 random curves in this fashion (under the assumption that two separate random searches would not check any of the same curves), none were found to have $a = 4$. While this does not definitively indicate the non-existence of such a curve, it does begin to seem possible that no hyperelliptic curves of genus 5 exist with $a = 4$ in characteristic 7.

FIGURE 4.4. Checking 10,000,000 random curves of genus 5 over $\mathbb{F}_{49}$ in Sage, under conditions that would force $a = 4$.

```
F=GF(49,'a')
R.<x>=PolynomialRing(F)
N=0
for i in range(10000000):
    m=random_vector(F,7)
    c2=m[0]
    c3=m[1]
    c4=m[2]
    c6=m[3]
    c7=m[4]
    c8=2*m[6]^3+5*m[5]*m[6]
    c9=m[5]
    c10=m[6]
    c5=2*c9^3+5*c8*c9*c10+6*c7*c10^2+6*c8^2+5*c7*c9+5*c6*c10
    c1=6*c7*c8^2+6*c7^2*c9+5*c6*c8*c9+6*c5*c9^2+5*c6*c7*c10+5*c5*c8*c10\
       +5*c4*c9*c10+6*c3*c10^2+6*c6^2+5*c5*c7+5*c4*c8+5*c3*c9+5*c2*c10
    if c2^3+6*c1*c2*c3+3*c1^2*c4==0:
        if c9^3+6*c8*c9*c10+3*c7*c10^2+3*c8^2+6*c7*c9+6*c6*c10+3*c5==0:
            if c3^3+6*c2*c3*c4+3*c1*c4^2+3*c2^2*c5+6*c1*c3*c5+6*c1*c2*c6\
               +3*c1^2*c7==0:
                if 3*c4^2*c5+3*c3*c5^2+6*c3*c4*c6+6*c2*c5*c6+3*c1*c6^2+3*\
                   c3^2*c7+6*c2*c4*c7+6*c1*c5*c7+6*c2*c3*c8+6*c1*c4*c8+3*\
                   c2^2*c9+6*c1*c3*c9+6*c1*c2*c10+3*c1^2==0:
                    if 3*c5^2*c6+3*c4*c6^2+6*c4*c5*c7+6*c3*c6*c7+3*c2*c7\
                       ^2+3*c4^2*c8+6*c3*c5*c8+6*c2*c6*c8+6*c1*c7*c8+6*c3\
                       *c4*c9+6*c2*c5*c9+6*c1*c6*c9+3*c3^2*c10+6*c2*c4*\
                       c10+6*c1*c5*c10+6*c2*c3+6*c1*c4==0:
                        if 3*c6*c7^2+3*c6^2*c8+6*c5*c7*c8+3*c4*c8^2+6*c5*\
                           c6*c9+6*c4*c7*c9+6*c3*c8*c9+3*c2*c9^2+3*c5^2*\
                           c10+6*c4*c6*c10+6*c3*c7*c10+6*c2*c8*c10+6*c1*\
                           c9*c10+6*c4*c5+6*c3*c6+6*c2*c7+6*c1*c8==0:
                            if 2*c2^2*c10^2+2*c1^2*c3*c10^2+2*c2^3*c9+2*\
                               c1^2*c3*c9-c1^3==0:
                                if c2^2*c10+c1*c3*c10+2*c1*c2==0:
                                    f=x^11+c10*x^10+c9*x^9+c8*x^8+c7*x^7+\
                                       c6*x^6+c5*x^5+c4*x^4+c3*x^3+c2*x\
                                       ^2+c1*x
                                    if f.is_squarefree()==True:
                                        C=HyperellipticCurve(f)
                                        B=C.Cartier_matrix()
                                        if B.determinant()==0:
                                            if B.rank()==1:
                                                N=N+1;
                                                [f,C.p_rank()]
N
0
```

For genus 6 curves, we saw in example 3.3.2 there are no smooth hyperelliptic curves of genus 6 with $a = 5$ when $p = 7$.

CHAPTER 5

Future Work

5.1. Lowering the bound

Without any known examples of algebraic curves of genus $g > 3$ with $a = g - 1$, it is unclear whether or not it is possible to lower the bound on the genus any further. Future work in this area could include further exploring the cases of $g = p - 1$ and $g = p - 2$. Examples 3.3.1 and 3.3.2 along with Theorem 3.3.9 suggest that curves with $a = g - 1$ likely do not exist when $g = p - 1$. As shown in Section 4.3, it seems possible that curves of genus 5 with $a = 4$ do not exist in characteristic 7. It would be worth generating data for $p = 11$ to see if the results agree. From there, an attempt could be made to make a general statement about the existence of such curves.

5.2. Ekedahl-Oort Types

At this point, the only examples we have of hyperelliptic curves with $a = g - 1$ are when $g = 3$. The next thing to consider for these curves, then, is what the Ekedahl-Oort types are for such curves. Since $a = 2$, we must have $f = 0$ or $f = 1$. The three possibilities for the Ekedahl-Oort type are [0 0 1], [0 1 1], and [1 1 1].

5.3. Non-Hyperelliptic Curves

While this paper explores the bound on the genus for hyperelliptic curves with $a = g - 1$, we could also ask how optimal the bound is on general algebraic curves with $a = g - 1$. Since we know algebraic curves of genus 3 exist with $a = 2$, the first interesting case is $g = 4$. Non-hyperelliptic curves of genus 4 are either conical or hyperboloidal. To consider allowed

a-numbers for such a curve X, we would need to first find a basis for $H^0(X, \Omega^1_X)$, and then determine how the Cartier operator acts on the basis elements.

Bibliography

[Car58] Pierre Cartier. Questions de rationalité des diviseurs en géométrie algébrique. *Bulletin de la Société Mathématique de France*, 86:177–251, 1958.

[Eke87] Torsten Ekedahl. On supersingular curves and abelian varieties. *Mathematica Scandinavica*, 60:151–178, 1987.

[Elk11] Arsen Elkin. The rank of the cartier operator on cyclic covers of the projective line. *Journal of Algebra*, 327(1):1–12, 2011.

[EP07] Arsen Elkin and Rachel Pries. Hyperelliptic curves with a-number 1 in small characteristic. *Albanian J. Math*, 1(4):245–252, 2007.

[Joh07] Otto Johnston. A note on the a-numbers and p-ranks of kummer covers. *arXiv preprint arXiv:0710.2120*, 2007.

[LO98] Ke-Zheng Li and Frans Oort. *Moduli of supersingular abelian varieties*, volume 1680. Springer, 1998.

[Oda69] Tadao Oda. The first de rham cohomology group and dieudonné modules. *Ann. Sci. École Norm. Super*, 4(2):63–135, 1969.

[Oor75] Frans Oort. Which abelian surfaces are products of elliptic curves? *Mathematische Annalen*, 214(1):35–47, 1975.

[Re01] Riccardo Re. The rank of the cartier operator and linear systems on curves. *Journal of Algebra*, 236(1):80–92, 2001.

[Tat97] John Tate. Finite flat group schemes. In *Modular forms and Fermats last theorem*, pages 121–154. Springer, 1997.

[Yui78] Noriko Yui. On the jacobian varieties of hyperelliptic curves over fields of characteristic p > 2. *Journal of Algebra*, 52(2):378–410, 1978.