



2009

The 2-Ranks of Hyperelliptic Curves with Extra Automorphisms

Darren B. Glass
Gettysburg College

Follow this and additional works at: <https://cupola.gettysburg.edu/mathfac>

 Part of the [Mathematics Commons](#)

Share feedback about the accessibility of this item.

Glass, Darren B. "The 2-ranks of Hyperelliptic Curves With Extra Automorphisms" *International Journal of Number Theory* 2009. 5(5):1-14

This is the author's version of the work. This publication appears in Gettysburg College's institutional repository by permission of the copyright owner for personal use, not for redistribution. Cupola permanent link: <https://cupola.gettysburg.edu/mathfac/20>

This open access article is brought to you by The Cupola: Scholarship at Gettysburg College. It has been accepted for inclusion by an authorized administrator of The Cupola. For more information, please contact cupola@gettysburg.edu.

The 2-Ranks of Hyperelliptic Curves with Extra Automorphisms

Abstract

This paper examines the relationship between the automorphism group of a hyperelliptic curve defined over an algebraically closed field of characteristic two and the 2-rank of the curve. In particular, we exploit the wild ramification to use the Dering-Shafarevich formula in order to analyze the ramification of hyperelliptic curves that admit extra automorphisms and use this data to impose restrictions on the genera and 2-ranks of such curves. We also show how some of the techniques and results carry over to the case where our base field is of characteristic $p > 2$.

Keywords

automorphism groups, hyperelliptic curves, p-ranks, wild ramification

Disciplines

Mathematics

THE 2-RANKS OF HYPERELLIPTIC CURVES WITH EXTRA AUTOMORPHISMS

Darren B Glass

Department of Mathematics, Gettysburg College, Gettysburg PA 17325
dglass@gettysburg.edu

Abstract

This paper examines the relationship between the automorphism group of a hyperelliptic curve defined over an algebraically closed field of characteristic two and the 2-rank of the curve. In particular, we exploit the wild ramification to use the Deuring-Shafarevich formula in order to analyze the ramification of hyperelliptic curves that admit extra automorphisms and use this data to impose restrictions on the genera and 2-ranks of such curves. We also show how some of the techniques and results carry over to the case where our base field is of characteristic $p > 2$.

1 Introduction

It is well known that curves in characteristic p which have maximal automorphism groups must have no nontrivial p -torsion points in their Jacobian variety [10]. Many arithmetic geometers believe that this result should generalize and that curves which admit many automorphisms should in general have small p -rank. The philosophy is that the automorphisms would have to permute the p -torsion points and therefore this would lead to a strong restriction on the p -rank, but this idea has never been precisely put into the form of a conjecture or theorem.

Several attempts (see [1], [4], [8], [12], [13] and others) have been made to investigate the relationship between automorphism groups and p -ranks. In [13], Zhu shows that there are hyperelliptic curves of every 2-rank that have automorphism group precisely $\mathbb{Z}/2\mathbb{Z}$. In this note, we examine the complementary case where we look at hyperelliptic curves which do admit non-hyperelliptic automorphisms. In particular, we will show that having an automorphism of odd degree m puts restrictions on the relationships between the genus and the 2-rank mod m .

It is well known that if a hyperelliptic curve in characteristic zero admits an extra (nonhyperelliptic) automorphism of order m then this places a restriction on the genus of the curve. (For details, we refer the reader to the tables of possible automorphism groups of hyperelliptic curves given by Shaska in [9]). We show that a similar result holds in characteristic two and that for each of the possible genera there will be a single possibility for the 2-rank mod m . As an application of these results we will be able to obtain the following corollaries as well as other similar results.

Corollary 1.1. *For each of the following pairs (g, σ) all hyperelliptic curves of genus g and 2-rank σ have automorphism group exactly $\mathbb{Z}/2\mathbb{Z}$ (ie they do not*

admit any extra automorphisms):

$$(2, 1), (4, 1), (6, 5), (6, 3), (8, 7), (8, 3), (8, 1), (10, 5)$$

For all other pairs (g, σ) with $g \leq 10$ there are hyperelliptic curves of genus g and 2-rank σ which admit extra automorphisms.

One notes that all of the pairs listed in Corollary 1.1 have g even and σ odd. This is not a coincidence, as the following corollary shows.

Corollary 1.2. *Let $0 < \sigma \leq g$ and let g be odd or let σ be even (or both). Then there exist hyperelliptic curves of genus g and 2-rank σ which admit extra automorphisms. In particular, if g and σ are both odd then there are curves whose automorphism group is $(\mathbb{Z}/2\mathbb{Z})^2$ and if σ is even then there are curves whose automorphism group contains $\mathbb{Z}/4\mathbb{Z}$ regardless of g .*

For most of this paper, we will assume that k is an algebraically closed field of characteristic 2 and consider hyperelliptic curves defined over such fields. We are interested in understanding the genus and the 2-rank of X , and in order to do this we analyze the ramification of the hyperelliptic map $X \rightarrow \mathbb{P}^1$. Recall that a hyperelliptic curve C in characteristic two can be defined by the Artin-Schreier equation $y^2 + y = f(x)$ where $f(x)$ is a rational function. Assume $f(x)$ has k poles given by x_1, \dots, x_k and let n_i be the order of the pole at x_i . Without any loss of generality, we can assume that all of the n_i are odd and, in this case, the genus of C is given by the formula $-1 + \frac{1}{2} \sum (n_i + 1)$ and the 2-rank of C is given by $k - 1$ due to the Riemann-Hurwitz and Deuring-Shafarevich formulae.

We also wish to recall some definitions and facts related to ramification of curves. Given a map $\phi : X \rightarrow Y$ with points $x \in X$ and $y \in Y$ such that $\phi(x) = y$, we let $e(x|y)$ be the ramification index. Furthermore, let $d(x|y)$ be the degree of the ramification divisor at y ; in particular, if $e(x|y)$ is not a multiple of p the ramification is tame and $d(x|y) = e(x|y) - 1$. Otherwise, the ramification is said to be wild and we have that $d(x|y) \geq e(x|y)$. It is well known (see [11], III.4.11 for one proof) that if we have a tower of points lying above each other that we can compute all of the ramification degrees by the formula $d(x|z) = d(x|y) + e(x|y)d(y|z)$.

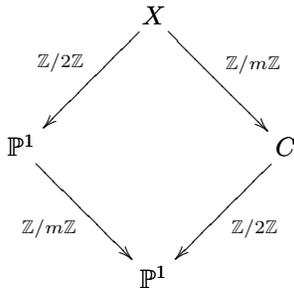
The next two sections look at the possible extra automorphisms that such a hyperelliptic curve might have. In Section 2 we consider the case of extra automorphisms of odd order and in Theorem 2.1 we show precise conditions on g and σ under which there will be a hyperelliptic curve of genus g and 2-rank σ which admit an extra automorphism of a given odd order. Section 3 considers the case of extra automorphisms of even order, and we obtain similar results after showing that the only possibilities are to admit extra involutions or extra automorphisms whose square is the hyperelliptic involution. In Section 4 we discuss the more general question of which automorphism groups can occur for hyperelliptic curves in characteristic two and then combine these results with results of the previous sections to discover which automorphism groups occur for small σ .

The techniques in Sections 2 and 3 rely on the fact that the hyperelliptic map was wildly ramified allowing us to use the Deuring-Shafarevich formula in order to determine the 2-rank. In section 5 we consider the case where k is an algebraically closed field of characteristic $p > 2$. In order to use the Deuring-Shafarevich formula we again must have wild ramification and therefore we consider only the case where our hyperelliptic curve has an extra automorphism of order p . Theorem 5.2 gives precise conditions on the p -rank under which this situation will occur.

The author would like to thank R. Pries and H. Zhu for helpful comments on this work.

2 Extra Automorphisms of Odd Order

Let X be a hyperelliptic curve defined over an algebraically closed field of characteristic two and let τ be an automorphism of odd degree m on X . Because the hyperelliptic involution is in the center of the automorphism group of X , τ induces an automorphism $\bar{\tau}$ on \mathbb{P}^1 which is also of degree m . Therefore, we are in the situation of the diagram below.



Because $\bar{\tau}$ gives a map from \mathbb{P}^1 to \mathbb{P}^1 of odd (and thus relatively prime to the characteristic of the base field) order, this covering must be ramified at two points, and totally ramified at each of these points. In particular, after a change of coordinates we may assume that $\bar{\tau}$ is branched at 0 and ∞ and thus that there is a unique point $0'$ (resp. ∞') lying above 0 (resp. ∞).

Let $D \subset \mathbb{P}^1$ be the branch locus of the hyperelliptic map $C \rightarrow \mathbb{P}^1$. In particular, if C is defined by the equation $y^2 + y = f(x)$ then D is the set of poles of $f(x)$. If $0 \in D$ then there must be a point $0_C \in C$ which lies above it, and by definition we compute that $e(0_C|0) = 2$ and $d(0_C|0) = n_0 + 1$ where n_0 is the degree of the pole of f at 0. One can now conclude that there must be a unique point in X (which we will denote by 0_x) lying over 0, and that $e(0_x|0_C) = m$ and thus $d(0_x|0_C) = m - 1$. Recall that we have the formula $d(x|z) = d(x|y) + e(x|y)d(x|z)$. Applying this to our situation above we can see that

$$\begin{aligned}
d(0_X|0) &= d(0_X|0_C) + e(0_X|0_C)d(0_C|0) \\
&= (m-1) + m(n_0+1) \\
&= mn_0 + 2m - 1
\end{aligned}$$

On the other hand, if we look at the tower on the left side of the diagram we see that $d(0_X|0) = d(0_X|0') + e(0_X|0')d(0'|0)$. However, we know that $d(0'|0) = m-1$ and $e(0_x|0') = 2$ and therefore we calculate

$$\begin{aligned}
mn_0 + 2m - 1 &= d(0_X|0) \\
&= d(0_X|0') + e(0_X|0')d(0'|0) \\
&= d(0_X|0') + 2m - 2
\end{aligned}$$

and therefore $d(0_X|0') = mn_0 + 1$. Similarly, if $\infty \in D_1$ we see that $d(\infty_X|0') = mn_\infty + 1$, where the notation is obvious.

Next, we note that if $x \neq 0, \infty$ and $x \in D_1$ then there will be m points of \mathbb{P}^1 which lie above x , and each of these points \tilde{x} will be a ramification point of the hyperelliptic map $X \rightarrow \mathbb{P}^1$. Furthermore, the ramification degree of these points will be the same as the ramification degree of the map $C \rightarrow \mathbb{P}^1$ at x .

In particular, if 0 and ∞ are not in D_1 so that $D_1 = \{x_1, \dots, x_k\}$ with the order of the pole at x_i equal to n_i then the hyperelliptic map is ramified at $mk = m(k-1) + m$ points and therefore that $\sigma_X = m\sigma_C + m - 1$. We then compute:

$$\begin{aligned}
g_X &= -1 + m \sum_{i=1}^k \frac{n_i + 1}{2} \\
&= -1 + m + m \left(-1 + \sum_{i=1}^k \frac{n_i + 1}{2} \right) \\
&= mg_C + m - 1
\end{aligned}$$

Next we assume that $0 \in D_1$ but $\infty \notin D_1$. Then the ramification points of the hyperelliptic map $X \rightarrow \mathbb{P}^1$ now include a single point which is a pole of order mn_0 and $m(k-1)$ points, m of which are poles of order n_i for $i = 1, \dots, k-1$. This gives a total of $m(k-1) + 1$ poles, so $\sigma_X = m(k-1) = m\sigma_C$. We compute the genus as follows:

$$\begin{aligned}
g_X &= -1 + \frac{mn_0 + 1}{2} + m \sum_{i=1}^{k-1} \frac{n_i + 1}{2} \\
&= -1 + \frac{-m + 1}{2} + m \sum_{i=0}^{k-1} \frac{n_i + 1}{2} \\
&= \frac{m-1}{2} + m \left(-1 + m \sum_{i=0}^{k-1} \frac{n_i + 1}{2} \right) \\
&= mg_C + \frac{m-1}{2}
\end{aligned}$$

It is clear that it is only the number and type of ramification points which enter into these calculations, so the case where $0 \notin D_1$ but $\infty \in D_1$ will give identical results.

It remains to consider the case where both 0 and ∞ are ramification points of the hyperelliptic map $C \rightarrow \mathbb{P}^1$. In this case, one sees that the ramification divisor of the hyperelliptic map $X \rightarrow \mathbb{P}^1$ will consist of poles at $0'$ and ∞' of orders mn_0 and mn_∞ respectively, as well as m poles each of order n_i for $i = 1, \dots, k-2$. This gives a total of $m(k-2) + 2 = m(k-1) - m + 2$ poles so that $\sigma_X = m\sigma_C - m + 1$. The genus calculation is similar to the above cases:

$$\begin{aligned}
g_X &= -1 + \frac{mn_\infty + 1}{2} + \frac{mn_0 + 1}{2} + m \sum_{i=1}^{k-2} \frac{n_i + 1}{2} \\
&= -1 + 1 - m + m \sum_{i=0, \dots, k-2, \infty} \frac{n_i + 1}{2} \\
&= m \left(-1 + \sum_{i=0, \dots, k-2, \infty} \frac{n_i + 1}{2} \right) \\
&= mg_C
\end{aligned}$$

These are the only cases possible, and therefore we have proven the ‘necessary’ conditions of the main result of this section:

Theorem 2.1. *Let X be a hyperelliptic curve defined over an algebraically closed field of characteristic 2 which has an extra automorphism of odd degree m . Let g be the genus of X and let σ be its 2-rank. Then one of the following three cases occurs.*

- i) $g \equiv \sigma \equiv m - 1 \pmod{m}$
- ii) $g \equiv \frac{m-1}{2}$ and $\sigma \equiv 0 \pmod{m}$
- iii) $g \equiv 0$ and $\sigma \equiv 1 \pmod{m}$

Furthermore, for any pair (g, σ) with $g \geq \sigma$ satisfying the above conditions there is a hyperelliptic curve with genus g , 2-rank σ , and automorphism group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

It remains to show the sufficiency of these conditions, and that we can construct a curve with automorphism group exactly $\mathbb{Z}/2m\mathbb{Z}$. To do this, we recall Zhu's result in [13] that there exist hyperelliptic curves $C \rightarrow \mathbb{P}^1$ of every possible 2-rank which admit no extra automorphisms. Furthermore, we can choose without any loss of generality whether or not 0 or ∞ will be in their branch locus. By taking the fibre product of these curves with the m -cyclic covers $\mathbb{P}^1 \rightarrow \mathbb{P}^1$ we obtain all possibilities.

We note the following corollary of this result which will be useful in Section 3.

Corollary 2.2. *Let m be an odd integer greater than one. There are no maps from \mathbb{P}^1 to \mathbb{P}^1 of order $2m$.*

Proof. Assume that there is a $\mathbb{Z}/2m\mathbb{Z}$ cover from X to \mathbb{P}^1 . Every $\mathbb{Z}/2m\mathbb{Z}$ cover is the fibre product of a degree m cover $f : Y \rightarrow \mathbb{P}^1$ with a degree 2 cover $g : C \rightarrow \mathbb{P}^1$. If the genus of X is zero then the genus of Y must also be zero and thus X is hyperelliptic. It follows that we are in the situation of the above Theorem. Furthermore, we note that if the genus of C is zero then the map from C to \mathbb{P}^1 must be branched at a single point (which eliminates the possibility that we are in the third case of Theorem 2.1). It follows from the proof of Theorem 2.1 that we must have either $g_X = mg_C + \frac{m-1}{2}$ or $g_X = mg_C + m - 1$ both of which are contradictions as $g_X = g_C = 0$ and $m > 1$. \square

3 Extra Automorphisms of Even Order

In this section we consider hyperelliptic curves that have extra automorphisms whose order is a power of two. We start by looking at curves with nonhyperelliptic involutions.

Theorem 3.1. *Let X be a hyperelliptic curve of genus g_X and 2-rank σ_X . Furthermore, assume that there is an involution other than the hyperelliptic involution in $\text{Aut}(X)$. Then $g_X \equiv \sigma_X \pmod{2}$. Conversely, if $g \equiv \sigma \pmod{2}$ then there exist hyperelliptic curves X with automorphism group $(\mathbb{Z}/2\mathbb{Z})^2$ such that $g_X = g$ and $\sigma_X = \sigma$.*

One proof of this result is given in [3]. Here, we give a different proof along the lines of the previous section.

Proof. It is well known that the hyperelliptic involution ρ will commute with any other automorphism and, therefore, if X admits an extra involution τ then the product $\tau\rho$ will also be an involution and therefore we have (at least) two nonhyperelliptic involutions. In [4], we showed with Pries that it follows from results of Kani and Rosen in [6] along with the Riemann-Hurwitz formula that

without loss of generality we may assume that either $g(X/\tau) = \frac{g(X)+1}{2}$ (in which case the map $X \rightarrow X/\tau$ has no ramification points) or $g(X/\tau) = \frac{g(X)}{2}$ (in which case the cover $X \rightarrow X/\tau$ has a single ramification point whose ramification degree is 2). As in the previous section, τ will induce an involution $\bar{\tau}$ on \mathbb{P}^1 . We note that it follows from the Riemann-Hurwitz formula that $\bar{\tau}$ must be ramified at a single point and without loss of generality we assume that the ramification point is ∞ . Furthermore, if ∞' denotes the unique point lying above ∞ we note that we must have that $d(\infty'|\infty) = e(\infty'|\infty) = 2$.

As above we now look separately at two cases depending on whether ∞' is a ramification point of the hyperelliptic map $X \rightarrow \mathbb{P}^1$. First, we assume that ∞' is not a ramification point of this map, so that the only ramification points of the hyperelliptic map $X \rightarrow \mathbb{P}^1$ are the pairs of points x'_i, x''_i lying above each of the ramification points $x_i \in D_1$. Furthermore, x_i, x'_i , and x''_i all have the same ramification degrees and therefore one can easily compute that $g_X = 2g_{X/\tau} + 1$ and $\sigma_X = 2\sigma_{X/\tau} + 1$. In particular, both g_X and σ_X are odd and we can construct any such pair by choosing C

For the second case, we assume that ∞' is a ramification point of the hyperelliptic map $X \rightarrow \mathbb{P}^1$. In that case one can see that $e(\infty_X|\infty) = 4$ and therefore that not only is there a unique point of X/τ (which we denote by ∞_τ) lying above ∞ but also that ∞_τ is a ramification point of the map $X \rightarrow X/\tau$. In particular, we note that if the map $X/\tau \rightarrow \mathbb{P}^1$ has k ramification points then the hyperelliptic map $X \rightarrow \mathbb{P}^1$ has $2(k-1) + 1$, so $\sigma_X = 2\sigma_{X/\tau}$. We can now compute that on one hand $d(\infty_X|\infty) = d(\infty_X|\infty') + 4$ but on the other hand it is equal to $d(\infty_X|\infty_\tau) + 2(n_\infty + 1)$ where n_∞ is the degree of the pole of $X/\tau \rightarrow \mathbb{P}^1$ at ∞ . Recalling from above that we could assume that $d(\infty_X|\infty_\tau) = 2$, we can conclude that $d(\infty|\infty') = 2n_\infty$. We next note that the hyperelliptic map $X \rightarrow \mathbb{P}^1$ will have 2 poles each of orders n_1, \dots, n_{k-1} and a single pole of order $2n$. Therefore we can carry through calculations like those in the proof of Theorem 2.1 to see that $g_X = 2g_{X/\tau}$. \square

Next, we wish to consider the case where X admits an extra automorphism of order 2^k . In order to do this, we first note the following result.

Lemma 3.2. *If k is a field of characteristic 2 then there are no $\mathbb{Z}/2^k\mathbb{Z}$ maps from \mathbb{P}^1 to \mathbb{P}^1 if $k \geq 2$.*

Proof. The Riemann-Hurwitz formula implies that if such a map existed then it would be ramified at a single point, which we may assume without any loss of generality is the point at ∞ . Therefore, the map is a map from $\mathbb{P}^1 \rightarrow \mathbb{P}^1$ which preserves ∞ and hence can be expressed as a linear transformation $x \mapsto ax + b$ for some a, b . Assume that this map is of order 2^k . Then $a^{2^k} = 1$ and, because the characteristic of our base field is two, we conclude that $a = 1$. However, the fact that $2b = 0$ now implies that the map is of order at most two. In particular, we conclude that there are no such maps if $k \geq 2$. \square

Now, assume that X has an extra automorphism τ of order 2^k . Then either τ induces an automorphism of order 2^k on \mathbb{P}^1 or else $\tau^{2^{k-1}}$ is itself the hyperelliptic

involution in which case τ induces an automorphism of order 2^{k-1} on \mathbb{P}^1 . By the above lemma, k must be one in the former case (in which case we are in the situation of Theorem 3.1), and in the latter case k must be equal to 2, in which case we have the following theorem.

Theorem 3.3. *There exist hyperelliptic curves with genus g and 2-rank σ and which have an extra automorphism of order four whose square is the hyperelliptic involution if and only if $\sigma > 0$ is even and $g > \sigma$ or $\sigma = 0$ and $g = 1$ or 2.*

Proof. Assume X is a hyperelliptic curve which admits an automorphism τ of order 4 such that τ^2 is the hyperelliptic involution. Without loss of generality, we may assume that X is defined by the equation $y^2 + y = f(x)$ so that the hyperelliptic map sends x to x and y to $y + 1$. The $\mathbb{Z}/4\mathbb{Z}$ map $X \rightarrow \mathbb{P}^1$ induced by τ must have a single point of ramification index 4 because the map $\mathbb{P}^1 \cong X / \langle \tau^2 \rangle \rightarrow X / \langle \tau \rangle \cong \mathbb{P}^1$ is only ramified at a single point. The other m ramification points (if they exist) will have ramification index 2 and therefore we can use the Deuring-Shafarevich formula to compute:

$$\begin{aligned} \sigma_X &= 1 + \#\mathbb{Z}/4\mathbb{Z}(\sigma_{\mathbb{P}^1} - 1 + \sum (1 - \frac{1}{p^e})) \\ &= 1 + 4(-1 + \frac{3}{4} + m\frac{1}{2}) \\ &= 2m \end{aligned}$$

and therefore σ_X is even.

We proceed by constructing examples of curves where such a map τ exists. If g is odd and $2 \leq \sigma = 2k < g$ is even we note that we can choose points x_1, \dots, x_k and positive integers a_1, \dots, a_k so that the curve X defined by the equation

$$y^2 + y = x^3 + \sum_{i=1}^k \left(\frac{1}{(x - x_i)^{a_i}} + \frac{1}{(x - x_i - \alpha)^{a_i}} \right)$$

has genus g and 2-rank σ . Moreover, the map defined by $\tau(x) = x + 1, \tau(y) = x + y + \zeta_3$ (where ζ_3 is a primitive cube root of 1) will be an automorphism of X such that τ^2 is the hyperelliptic involution. If $g = 1$ and $\sigma = 0$ the curve defined by $y^2 + y = x^3$ similarly satisfies the desired conditions.

On the other hand, if g is even and $2 \leq \sigma = 2k < g$ is even then we similarly define X by the equation

$$y^2 + y = x^3 + \sum_{i=1}^k \left(\frac{1}{(x - x_i)^{a_i}} + \frac{1}{(x - x_i - \alpha)^{a_i}} \right)$$

In this case, the map defined by $\tau(x) = x + 1, \tau(y) = y + x^2$ will have the desired properties. If $g = 2$ and $\sigma = 0$, the curve defined by $y^2 + y = x^5 + x^3$ will fit the requirements.

It remains only to show that if a hyperelliptic curve is ordinary then there can not be a map τ with τ^2 being the hyperelliptic involution. Recall that a

hyperelliptic curve in characteristic two is ordinary if it is of the form $y^2 + y = f(x)$ where $f(x)$ has only simple poles. If τ^2 is hyperelliptic then $\tau(x) = x + \gamma$ for some γ and thus without loss of generality the poles consist of $\{\infty, \alpha_1, \alpha_1 + \gamma, \dots, \alpha_k, \alpha_k + \gamma\}$. Given that $\tau(y) = y + B(x)$ for some function $B(x)$ we now get that $(B(x))^2 + B(x) + ax + a\gamma = ax$ for some a and this is a contradiction. \square

We wish to show that we do not need to consider any other cases of automorphisms of even order. In particular, let us assume that a hyperelliptic curve X admits an automorphism of degree $2^k m$ where m is an odd number. We begin by noting that any such cover $X \rightarrow C$ can be broken down as the composition of two covers $X \rightarrow D \rightarrow C$ where $X \rightarrow D$ is a $\mathbb{Z}/m\mathbb{Z}$ cover and $D \rightarrow C$ is a $\mathbb{Z}/2^k\mathbb{Z}$ cover. As in the above, all of these maps induce maps on \mathbb{P}^1 and we get a tower of extensions. However, we note that if $k \geq 2$ then there are no $2^k m$ -cyclic automorphisms of \mathbb{P}^1 and so we do not need to consider this case.

If $k = 1$ then we have an extra automorphism τ of order $2m$. One possibility is that τ^m is the hyperelliptic involution, and this is the situation covered in Theorem 2.1. It therefore will suffice to consider the case where τ^m is not the hyperelliptic involution, in which case it will induce an automorphism of order $2m$ on \mathbb{P}^1 . Corollary 2.2 tells us that there are no $2m$ -cyclic automorphisms of \mathbb{P}^1 , so this case cannot occur. Thus, the only possible extra automorphisms of even order in characteristic two are of order two, order four (in which case τ^2 is hyperelliptic) or $2m$ where m is odd and τ^m is hyperelliptic.

4 Possible Automorphism Groups

This section will combine the results of the previous two sections in an attempt to answer the question of what automorphism groups can occur for a given genus and a given 2-rank. Where possible, we will also give equations of such curves.

Recall from Corollary 2.2 and Lemma 3.2 that the only cyclic maps from $\mathbb{P}^1 \rightarrow \mathbb{P}^1$ are of order two or odd order. Recalling from [5] that there are no hyperelliptic curves with $(\mathbb{Z}/2\mathbb{Z})^k$ as a subgroup of their automorphism group, we note that the abelian possibilities for the automorphism groups that remain possible are the following: $(\mathbb{Z}/2\mathbb{Z})^2, (\mathbb{Z}/2\mathbb{Z})^3, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2m\mathbb{Z}$. Furthermore, we note that Theorem 2.1 gives explicit conditions on the genus and 2-rank under which $\mathbb{Z}/2m\mathbb{Z}$ will occur as an automorphism group of a hyperelliptic curve, and Theorems 3.1 and 3.3 do the same for $(\mathbb{Z}/2\mathbb{Z})^2$ and $\mathbb{Z}/4\mathbb{Z}$ respectively. The following theorem treating the remaining case follows immediately from results in [3].

Theorem 4.1. *There are hyperelliptic curves of genus g and 2-rank σ with automorphism group $(\mathbb{Z}/2\mathbb{Z})^3$ if and only if either $g \equiv \sigma \equiv 0$ or $g \equiv \sigma \equiv 3$ (mod 4)*

The structure of the possible nonabelian automorphism groups in characteristic zero are discussed by Shaska in [9] and in characteristic $p > 2$ in [2]

and [7], and there are a similar number of possibilities in characteristic two. Distinguishing between these automorphism groups is trickier in general, and for large σ one must keep track of a number of ramification types. However, for small 2-ranks one can examine the situation quite explicitly and we do this in the remainder of this section. If $\sigma = 0$ then our curve will be ramified at a single point which we may assume without loss of generality is ∞ . Theorem 2.1 implies that we can have extra automorphisms of odd order m if and only if $m|2g+1$. In particular, for any such m the curve defined by the equation $y^2 + y = x^{2g+1} + x^m$ will have automorphism group precisely $\mathbb{Z}/2m\mathbb{Z}$. Furthermore, Theorem 3.1 tells us that if g is even then we may have extra involutions which will not commute with any automorphisms of odd order. Thus, the possible automorphism groups for odd g are $\mathbb{Z}/2m\mathbb{Z}$ where $m|2g+1$ and for even g are $\mathbb{Z}/2m\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2$, and a nonabelian group of order $4m$. We note that this is the same case considered by Lehr and Matignon in [8] using different techniques.

If $\sigma = 1$ then by Theorem 2.1 there will be curves with an extra automorphism of odd order m for all $m|g$ and and if g is odd there will be curves with extra involutions. The curve X will be defined by $y^2 + y = f(x)$ where $f(x)$ has two poles which we may assume are at 0 and ∞ . Because we are working over a field of characteristic 2, if there is an extra involution then it must permute these two points and therefore they must have poles of the same order. In particular, this implies that if there is also an extra automorphism of odd order then it will be of order g and one can easily check that the extra automorphism of order m cannot commute with the extra involution as the latter sends $x \rightarrow \frac{1}{x}$ while the former sends $x \rightarrow \zeta x + \beta$ where $\zeta^m = 1$ but $\zeta \neq 1$. Therefore, we are left with the following possible automorphism groups:

Group	Sample Curve	Condition on g
$\mathbb{Z}/2m\mathbb{Z}$, $m g$ m odd	$y^2 + y = x^m + \frac{1}{x^{2g-m}}$	all g
$\mathbb{Z}/2g\mathbb{Z}$	$y^2 + y = x^g + \frac{a}{x^g}$, $a \neq 1, 0$	g odd
$(\mathbb{Z}/2\mathbb{Z})^2$	$y^2 + y = x^g + x + \frac{1}{x^g} + \frac{1}{x}$	g odd
Nonabelian	$y^2 + y = x^g + \frac{1}{x^g}$	g odd

If $\sigma = 2$ then it follows from the theorems of the earlier sections that the only possible extra automorphisms are of order 3 (if $3|g+1$), order 2 (if g is even) and order 4 (whose square is hyperelliptic). Each of these types of automorphisms occur, and it follows from our above constructions and the results of Zhu in [13] that we can construct hyperelliptic curves of the appropriate genera which have automorphism group *exactly* $\mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2$, $\mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/6\mathbb{Z}$. We are left to consider which of them can occur simultaneously. If X has an automorphism τ of order three then it follows from Theorem 2.1 that $C = X / \langle \tau \rangle$ will have 2-rank equal to zero. In particular, C will not have any extra automorphisms of order 4 by Theorem 3.3. If g_C is even (and thus $g_X \equiv 2 \pmod{6}$) then C may have an extra involution. In this case, one can check that the extra involution cannot commute with τ . We summarize these results in the following table:

Group	Sample Curve	Condition on g
$\mathbb{Z}/2\mathbb{Z}$		all g
$\mathbb{Z}/4\mathbb{Z}$	$y^2 + y = x^g + \frac{1}{x^g}$	g odd
$\mathbb{Z}/6\mathbb{Z}$	$y^2 + y = x^a + \frac{1}{x^a} + \frac{1}{(x+1)^a}, a = \frac{g+1}{3}$	$3 g+1$
$(\mathbb{Z}/2\mathbb{Z})^2$	$y^2 + y = x^g + x + \frac{1}{x^g} + \frac{1}{x}$	g odd
Nonabelian		$g \equiv 2 \pmod{6}$

As we allow the 2-rank to get larger we will have more ramification points and therefore more poles which we will need to consider, making the analysis of possible automorphism groups more complicated. However, in principle for a fixed g and σ one should be able to construct all possible automorphism groups using the above techniques.

5 Characteristic $p > 2$

In this final section, we will consider the case where k is an algebraically closed field of characteristic $p > 2$. The results and techniques in the above sections relied on interpreting X as an Artin-Schreier cover of \mathbb{P}^1 , and thus we will only be able to consider the case where X is a hyperelliptic curve which admits an extra automorphism whose order is a multiple of p . However, it is easy to see that one can generalize the ideas behind Lemma 3.2 and Corollary 2.2 to prove the following:

Lemma 5.1. *If k is a field of characteristic p and $\tau : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ is a cyclic map of order m then either $\gcd(m, p) = 1$ or $m = p$.*

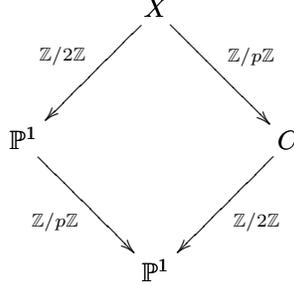
In particular, hyperelliptic curves defined in characteristic p can only admit extra automorphisms whose order is relatively prime to p , is equal to p or is equal to $2p$ and whose square is the hyperelliptic involution. In this note, we will only consider the latter two cases, which occur simultaneously.

Theorem 5.2. *Let X be a hyperelliptic curve defined over an algebraically closed field of characteristic $p > 2$ which admits an extra automorphism of degree p . Let g be the genus of X and let σ be its p -rank. Then one of the following two cases occurs.*

- i) $g \equiv \sigma \equiv p - 1 \pmod{p}$
- ii) $g \equiv \frac{p-1}{2}$ and $\sigma \equiv 0 \pmod{p}$

Furthermore, for any pair (g, σ) with $g \geq \sigma$ satisfying the above conditions there is a hyperelliptic curve whose automorphism group contains $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ with genus g and 2-rank σ .

Proof. let X be a hyperelliptic curve in characteristic p which admits an extra automorphism of order p . Then we will have the following diagram.



The map $\mathbb{P}^1 \rightarrow \mathbb{P}^1$ is ramified with ramification degree $2p - 2$ at a single point, which we may assume without any loss of generality is the point at ∞ . We denote the point lying above ∞ by ∞' . We wish to consider the ramification of the cover $X \rightarrow C$. Doing an analysis similar to that in previous sections, we can see that this cover will be ramified only at the point (or points) above ∞ and therefore we need to consider two separate cases.

First we assume that ∞ is in the branch locus of the hyperelliptic cover $C \rightarrow \mathbb{P}^1$ and thus there will be a single point ∞_C lying above it. As before, we note that in this case there will also be a single point $\infty_X \in X$ lying above ∞ . We compute:

$$\begin{aligned}
d(\infty_X | \infty_C) &= d(\infty_X | \infty) - e(\infty_X | \infty_C) d(\infty_C | \infty) \\
&= d(\infty_X | \infty) - p \\
&= d(\infty_X | \infty') + e(\infty_X | \infty') d(\infty' | \infty) - p \\
&= 1 + 2(2p - 2) - p \\
&= 3p - 3
\end{aligned}$$

In particular, the $\mathbb{Z}/p\mathbb{Z}$ -cover $X \rightarrow C$ will be ramified at a single point with ramification degree $3p - 3$. One can now use the Riemann-Hurwitz and Deuring-Shafarevich formulas to compute directly that $g_X = pg_C + \frac{p-1}{2}$ and $\sigma_X = p\sigma_C$.

Next, we wish to consider the case where ∞ is not in the branch locus of $C \rightarrow \mathbb{P}^1$. In this case, we can easily compute that the $\mathbb{Z}/p\mathbb{Z}$ -cover $X \rightarrow C$ will be ramified at both of the points that lie above ∞ and that for each of these points the ramification degree will be $2p - 2$. It is then an easy computation to see that $g_X = pg_C + p - 1$ and $\sigma_X = p\sigma_C + p - 1$.

In order to see the sufficiency of these conditions we note that it is shown in [4] that there exist hyperelliptic curves of every possible p -rank and without loss of generality we can let ∞ be ramified or unramified as necessary. By choosing C appropriately and then taking the fibre product with the $\mathbb{Z}/p\mathbb{Z}$ cover $\mathbb{P}^1 \rightarrow \mathbb{P}^1$ we will obtain a curve with the desired genus and p -rank, proving the result. \square

Remark 5.3. *In many of the theorems in the earlier sections we were able to exploit Zhu's result from [13] that there are hyperelliptic curves of every possible*

2-rank with no extra automorphisms in order to construct curves where we know the precise automorphism group. However, the results in [4] do not tell us what the automorphism group of the curves under consideration are, and therefore Theorem 5.2 is slightly weaker than the results of earlier sections because we do not know the full automorphism group of the curves we have constructed.

Remark 5.4. We note the similarity between Theorem 2.1 and Theorem 5.2. This leads us to believe that there is likely to be a purely geometric proof of these theorems which does not depend on the characteristic of the base field.

References

- [1] I. Bouw. The p -rank of ramified covers of curves. *Compositio Math.*, 126(3):295–322, 2001.
- [2] R. Brandt and H. Stichtenoth. Die Automorphismengruppen hyperelliptischer Kurven. *Manuscripta Math.*, 55(1):83–92, 1986.
- [3] D. Glass. Klein-four covers of the projective line in characteristic two. *Albanian J. Math.*, 1(1):3–11 (electronic), 2007.
- [4] D. Glass and R. Pries. Hyperelliptic curves with prescribed p -torsion. *Manuscripta Math.*, 117(3):299–317, 2005.
- [5] D. Glass and R. Pries. On the moduli space of Klein four covers of the projective line. In *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 58–70. World Sci. Publ., Hackensack, NJ, 2005.
- [6] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284(2):307–327, 1989.
- [7] A. Kontogeorgis. The group of automorphisms of cyclic extensions of rational function fields. *J. Algebra*, 216(2):665–706, 1999.
- [8] C. Lehr and M. Matignon. Automorphism groups for p -cyclic covers of the affine line. *Compos. Math.*, 141(5):1213–1237, 2005.
- [9] T. Shaska. Determining the automorphism group of a hyperelliptic curve. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, pages 248–254 (electronic), New York, 2003. ACM.
- [10] H. Stichtenoth. Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkörpern. *Arch. Math. (Basel)*, 24:615–631, 1973.
- [11] H. Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer-Verlag, Berlin, 1993.

- [12] D. Subrao. The p -rank of Artin-Schreier curves. *Manuscripta Math.*, 16(2):169–193, 1975.
- [13] H. J. Zhu. Hyperelliptic curves over \mathbb{F}_2 of every 2-rank without extra automorphisms. *Proc. Amer. Math. Soc.*, 134(2):323–331, 2006.