

The 2-ranks of Hyperelliptic Curves with Extra Automorphisms

Darren Glass

*Department of Mathematics, Gettysburg College
300 North Washington Street, Gettysburg, PA 17325
dglass@gettysburg.edu*

Received (Day Month Year)

Accepted (Day Month Year)

Communicated by xxx

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: Hyperelliptic curves; p -ranks; wild ramification; automorphism groups

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 [11]. 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], [9] [13], [16] and others) have been made to investigate the relationship between automorphism groups and p -ranks. While this is a difficult question in general, much can be said if one restricts their attention to the case where the characteristic of the base field is $p = 2$. In [16], 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 extra automorphism of 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 (non-hyperelliptic) 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

2 Darren Glass

hyperelliptic curves given by Shaska in [10]). 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. *Let g and σ be nonnegative integers with $\sigma \leq g$. Furthermore, assume that the following conditions all hold:*

- g is even.
- σ is odd.
- The quantities $2g + 1 - \sigma$ and $\sigma(\sigma^2 - 1)$ share no common odd factors.

Then all hyperelliptic curves with genus g and 2-rank σ have automorphism group exactly $\mathbb{Z}/2\mathbb{Z}$. Furthermore, if any of the above quantities fail then there exist hyperelliptic curves with genus g and 2-rank σ which do admit extra automorphisms.

In particular, for fixed odd $\sigma \geq 3$ there exists an integer N_σ and a nonempty set of congruence classes mod N_σ so that all hyperelliptic curves of 2-rank σ and genus g have automorphism group $\mathbb{Z}/2\mathbb{Z}$ if and only if g lies in one of these congruence classes. For example, if $\sigma = 3$ then $g \equiv 0, 2 \pmod{6}$ and if $\sigma = 5$ we have $g \equiv 0, 4, 6, 10, 16, 18, 24, 28 \pmod{30}$.

Corollary 1.2. *Let $0 < \sigma \leq g$ with g odd or σ even. 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 contains $(\mathbb{Z}/2\mathbb{Z})^2$ and if $\sigma > 0$ 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 [12], 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 3 we consider the case of extra automorphisms of odd order

and in Theorem 3.2 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 4 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 5 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 3 and 4 rely on the fact that the hyperelliptic map is wildly ramified allowing us to use the Deuring-Shafarevich formula in order to determine the 2-rank. In section 6 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 6.2 gives precise conditions on the p -rank under which this situation will occur.

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

2. Automorphism Groups of Hyperelliptic Curves

In this section we consider the possible automorphism groups of hyperelliptic curves over algebraically closed fields of characteristic two. The structure of the automorphism groups of hyperelliptic curves in characteristic zero are discussed in [10] and in characteristic $p > 2$ in [2] and [7], and the situation is similar but not identical in characteristic two. Most of the results of this section can be deduced from the results of Valentini and Madan in [14], but we will sketch different proofs in several cases.

Lemma 2.1. *A nontrivial cyclic Galois cover $\mathbb{P}_k^1 \rightarrow \mathbb{P}_k^1$ is isomorphic to either the $\mathbb{Z}/m\mathbb{Z}$ cover given by $x \mapsto x^m$ for m odd or the $\mathbb{Z}/2\mathbb{Z}$ cover $x \mapsto x^2 + x$.*

Proof.

We begin by considering automorphisms of \mathbb{P}^1 of odd degree m . In this case, all ramification is tame and therefore it follows from the Riemann-Hurwitz formula that such a cover must be totally ramified at two points and have no other ramification. In particular, the cover is isomorphic to the cover given by $x \mapsto x^m$.

We next consider automorphisms of \mathbb{P}^1 of order 2^ℓ . The Riemann-Hurwitz formula implies that if such an automorphism 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 automorphism can be expressed as a linear transformation $x \mapsto ax + b$ for some a, b . Then $a^{2^\ell} = 1$ 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 $\ell \geq 2$ and that if $\ell = 1$ then the cover is isomorphic to $x \mapsto x^2 + x$.

4 *Darren Glass*

Because of the above results, it remains only to consider the case of Galois covers of degree $2m$ where m is odd. It follows from the above that such a cover would be ramified at two points and the ramification type of the cover would be $(m, 2m)$. Thus, the generator g of the Galois group has g^2 fixing three points. In particular, g^2 is the identity map and therefore $m = 1$. \square

Because the hyperelliptic involution is central in the automorphism group of a hyperelliptic curve, we have the short exact sequence

$$1 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow \text{Aut}(X) \rightarrow \overline{\text{Aut}}(X) \rightarrow 1$$

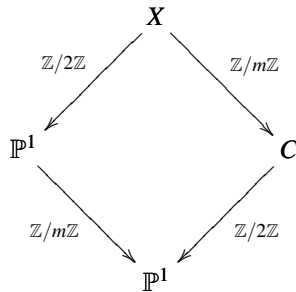
where $\overline{\text{Aut}}(X)$ is the reduced automorphism group. The following results about $\overline{\text{Aut}}(X)$ and $\text{Aut}(X)$ follow directly from Lemma 2.1 and [14][Thm 5] and will be useful to us in the following sections.

Theorem 2.2.

- (1) If $\overline{\text{Aut}}(X)$ is of odd order m then it is cyclic and $\text{Aut}(X) \cong \mathbb{Z}/2m\mathbb{Z}$.
- (2) The 2-Sylow subgroup of $\overline{\text{Aut}}(X)$ is elementary abelian.
- (3) $\overline{\text{Aut}}(X)$ is one of the following groups: $(\mathbb{Z}/2\mathbb{Z})^\ell$, $\mathbb{Z}/m\mathbb{Z}$ (for m odd), the dihedral group of order $2m$ (for odd m), A_4 , A_5 , $\text{PSL}_2(\mathbb{Z}/2\mathbb{Z})$, $\text{PGL}_2(\mathbb{Z}/2\mathbb{Z})$, or a semidirect product of $(\mathbb{Z}/2\mathbb{Z})^\ell$ with $\mathbb{Z}/m\mathbb{Z}$ where $m|2^\ell - 1$.
- (4) If τ is an element of $\text{Aut}(X)$ of even order $2n$ then τ is either of order 2 or τ^n is the hyperelliptic involution with $n = 2$ or n odd.

3. 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 ramified at 0 and ∞ .

Lemma 3.1. *Let $\psi : C \rightarrow \mathbb{P}^1$ be a hyperelliptic map with branch locus D and let X be the fiber product of ψ with the $\mathbb{Z}/m\mathbb{Z}$ -cover $\mathbb{P}^1 \rightarrow \mathbb{P}^1$ branched at 0 and ∞ . Let $k = \#D$ and $a = \#(\{0, \infty\} \cap D)$. Then*

- (1) $\sigma_X + 1 - a = m(\sigma_C + 1 - a)$
- (2) $2g_X + 2 - a = m(2g_C + 2 - a)$

Proof. To prove (i) we note that if $x \in D$ and $x \notin \{0, \infty\}$ then there will be m points of \mathbb{P}^1 which lie above x , and each of these points \bar{x} will be a ramification point of the hyperelliptic map $X \rightarrow \mathbb{P}^1$. Furthermore, for each point in $x \in \{0, \infty\} \cap D$ there is a unique point in \mathbb{P}^1 above x which will be a ramification point of $X \rightarrow \mathbb{P}^1$. In particular, the hyperelliptic map $X \rightarrow \mathbb{P}^1$ will be branched at $m(k - a) + a$ points and (i) follows.

We next wish to compare g_X and g_C . In particular, note that the map $X \rightarrow C$ is a $\mathbb{Z}/m\mathbb{Z}$ -cover of curves which will be branched at $(4 - a)$ points. The cover is tame, so the Riemann-Hurwitz formula implies that $2g_X - 2 = m(2g_C - 2) + (m - 1)(4 - a)$ from which (ii) immediately follows. \square

We are now ready to state the main result of this section.

Theorem 3.2. *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.*

- (1) $g \equiv \sigma \equiv m - 1 \pmod{m}$
- (2) $g \equiv \frac{m-1}{2}$ and $\sigma \equiv 0 \pmod{m}$
- (3) $g \equiv 0$ 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 containing $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Proof. As above, the fact that the hyperelliptic involution is in the center of the automorphism group of X implies that any other automorphism of X induces an automorphism of \mathbb{P}^1 and in particular we will be in the situation of Lemma 3.1. The lemma therefore implies the necessity of one of the above conditions, which correspond to the choice of $a \in \{0, 1, 2\}$.

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 [16] 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 fiber product of these curves with the m -cyclic covers $\mathbb{P}^1 \rightarrow \mathbb{P}^1$ we obtain all possibilities. \square

6 *Darren Glass*

4. Extra Automorphisms of Even Order

In this section we consider hyperelliptic curves that have extra automorphisms whose order is even. It follows from Theorem 2.2 that the only cases we need to consider are order two, order four, and order $2m$ where m is odd. The latter case was considered in the previous section. We continue by looking at curves which allow nonhyperelliptic involutions.

Lemma 4.1. *Let g and σ be integers with $0 \leq \sigma \leq g$ and $g \equiv \sigma \pmod{2}$. Then there exists a hyperelliptic curve X with genus g and 2-rank σ with automorphism group containing $(\mathbb{Z}/2\mathbb{Z})^2$.*

Proof. Assume that g and σ are both even integers. Let C be a hyperelliptic curve of genus $\frac{g-1}{2}$ and 2-rank $\frac{\sigma-1}{2}$ which is defined by the equation $y^2 + y = f(x)$, where $f(x)$ does not have a pole at ∞ . If one takes the fiber product of the hyperelliptic map $C \rightarrow \mathbb{P}^1$ with the map $\mathbb{P}^1 \rightarrow \mathbb{P}^1$ defined by the equation $x \mapsto x^2 + x$, then it follows from [15] that the resulting curve X will have genus g , 2-rank σ and a copy of $(\mathbb{Z}/2\mathbb{Z})^2$ in its automorphism group.

If g and σ are even integers, then we wish to do a similar construction. In particular, let C be a hyperelliptic curve of genus $\frac{g}{2}$ and 2-rank $\frac{\sigma}{2}$ which is defined by the equation $y^2 + y = f(x)$ where $f(x) + x$ has the same poles (with the same orders) as $f(x)$. (In particular, if $g \neq \sigma$ then one can choose $f(x)$ to have a pole of order greater than one at ∞ .) The same fibre product construction will now give us a curve with the desired properties. \square

Theorem 4.2. *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 containing $(\mathbb{Z}/2\mathbb{Z})^2$ such that $g_X = g$ and $\sigma_X = \sigma$.*

The sufficiency of the condition in the theorem is the content of Lemma 4.1. One proof of the necessity 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. As in the previous section, τ will induce an involution $\bar{\tau}$ on \mathbb{P}^1 . We note 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 ∞ in this cover we note that we must have that $d(\infty'|\infty) = e(\infty'|\infty) = 2$. As in the previous section, let us denote the curve $X / \langle \tau \rangle$ by C .

If g_X is odd then we showed with Pries in [4] that it follows from results in [6] along with the Riemann-Hurwitz formula that without loss of generality we may assume that $g_C = \frac{g_X+1}{2}$ and the map $X \rightarrow X/\tau$ has no ramification points. The fact that the map $X \rightarrow C$ is étale implies that ∞ is a ramification point of the map $C \rightarrow \mathbb{P}^1$ and that ∞' is not a ramification point of the hyperelliptic map $X \rightarrow \mathbb{P}^1$. In particular, the only ramification points of this map will be the pairs of points x'_i, x''_i lying above each of the finite ramification

points x_i of the hyperelliptic map $C \rightarrow \mathbb{P}^1$. Therefore we can compute that $\sigma_X + 1 = 2(\sigma_C)$ and in particular σ_X will be odd.

If g_X is even then the results of [4] imply that $g_C = \frac{g_X}{2}$ and the cover $X \rightarrow C$ has a single ramification point whose ramification degree is 2. Furthermore, this ramification point must be a branch point of the map $C \rightarrow \mathbb{P}^1$ and in particular must lie over ∞ . Comparing ramification degrees, this implies that ∞' must be a ramification point of the hyperelliptic map $X \rightarrow \mathbb{P}^1$ so we can compute that $\sigma_X + 1 = 2(\sigma_C) + 1$ so that σ_X is even. \square

The preceding theorem can be generalized in the following way to consider curves which admit multiple extra involutions.

Theorem 4.3. *There are hyperelliptic curves X of genus g and 2-rank σ such that $(\mathbb{Z}/2\mathbb{Z})^n \subseteq \text{Aut}(X)$ if and only if either $g \equiv \sigma \equiv 0$ or $g \equiv \sigma \equiv -1 \pmod{2^{n-1}}$*

Proof. Let X be a hyperelliptic curve containing $(\mathbb{Z}/2\mathbb{Z})^n$ in its automorphism group. Then in particular it can be viewed as a $(\mathbb{Z}/2\mathbb{Z})^n$ -cover of the projective line, and therefore as a fiber product of n hyperelliptic curves. Following the method of [5, Lemma 12], it is clear that $n-1$ of these covers must have the same single ordinary pole, which we may assume is at ∞ without any loss of generality. Furthermore, if the final hyperelliptic cover $\phi_n : C_n \rightarrow \mathbb{P}^1$ has genus g' and 2-rank σ' then X will either have genus $2^{n-1}g'$ and 2-rank $2^{n-1}\sigma'$ or genus $2^{n-1}g' - 1$ and 2-rank $2^{n-1}\sigma' - 1$, depending on whether or not ϕ_n is branched at ∞ in a way which will cause cancelation. For details, see [3, Cor. 4.11]. \square

Remark 4.4. We note that this is one place where the situation is quite different in characteristic two then when the characteristic unequal to two. In particular, if $p \neq 2$ then it is shown in [4, Cor. 1] that $(\mathbb{Z}/2\mathbb{Z})^n$ -covers of \mathbb{P}^1 only exist for curves with $g \equiv 1 \pmod{2^{n-2}}$ and in [5, Lemma 12] that curves which are both hyperelliptic and $(\mathbb{Z}/2\mathbb{Z})^n$ -covers of \mathbb{P}^1 only exist if $n \leq 3$.

The final case that we need to consider occurs when X is a hyperelliptic curve which admits an automorphism τ so that τ^2 is the hyperelliptic involution ι . We first consider the case where $\sigma = 0$.

Example 4.5. Let $g \geq 2$ be even and let

$$f(x) = x^{g+1} + (x+1)^{g+1} + (x+1)^g + x^g + x = \sum_{i=0}^g c_i x^i$$

Note that $f(x+1) + f(x) = 1$ so if τ is defined by $\tau(x) = x+1$ and $\tau(y) = y + f(x)$ then $\tau^2(x) = x$ and $\tau^2(y) = y + 1$.

Furthermore, note that $c_g = 1$, $c_1 = 0$, and for all $1 < i < g$ we have $c_i = \binom{g}{i-1}$. The fact that g is even implies that $c_i = 0$ if i is even and less than g . For all $0 \leq j \leq g$ define $\alpha_{2j+1} = c_j^2 + c_{2j} + c_{2j+1}$, with the convention that $c_i = 0$ for all $i > g$.

8 *Darren Glass*

Let X be the hyperelliptic curve defined by the equation $y^2 + y = h(x)$ where $h(x) = \alpha_{2g+1}x^{2g+1} + \dots + \alpha_1x$. We wish to check that τ is an automorphism of X . In particular, we notice that

$$\begin{aligned} \sum_{i=0}^g c_i^2 (x+1)^{2i+1} &= (x+1) \sum_{i=0}^g c_i^2 (x+1)^{2i} \\ &= (x+1)[f(x+1)]^2 \\ &= (x+1)([f(x)]^2 + 1) \\ &= \sum_{i=0}^g c_i^2 x^{2i+1} + \sum_{i=0}^g c_i^2 x^{2i} + x + 1 \end{aligned}$$

This fact allows us to show that $h(x+1) + h(x) = [f(x)]^2 + f(x)$ which implies that τ is an automorphism of X . Above, we computed that τ^2 acts as the hyperelliptic involution fixing x and sending y to $y + 1$.

Lemma 4.6. *There exist hyperelliptic curves with genus g and 2-rank 0 and which have an extra automorphism of order four whose square is the hyperelliptic involution if and only if $g \geq 2$ is even.*

Proof. Assume that X is a curve of genus g and 2-rank $\sigma = 0$. Without loss of generality, we may assume that X is defined by the equation $y^2 + y = x^{2g+1} + \alpha_{2g-1}x^{2g-1} + \dots + \alpha_1x$. Furthermore, let us assume that there is some automorphism τ so that τ^2 is the hyperelliptic involution. The fact that $\tau^2(x) = x$ implies that $\tau(x) = x + b$ for some b . Furthermore, without loss of generality $\tau(y) = y + c_g x^g + c_{g-1}x^{g-1} + \dots + c_1x + c_0$. The fact that $\tau^2 = \iota$ implies that

$$c_g[x^g + (x+b)^g] + c_{g-1}[x^{g-1} + (x+b)^{g-1}] + \dots + c_1[x + (x+b)] = 1 \quad (4.1)$$

and the fact that τ is an automorphism of X implies that

$$(y + c_g x^g + \dots + c_0)^2 + (y + c_g x^g + \dots + c_0) = (x+b)^{2g+1} + \dots + \alpha_1(x+b) \quad (4.2)$$

The constant term on the left hand side of Equation 4.1 is a multiple of b and we deduce that $b \neq 0$. Looking at the coefficient of x^{2g} on both sides of Equation 4.2 implies that $c_g^2 = b$ while comparing the coefficient of x^{g-1} on both sides of Equation 4.1 implies that $bgc_g = 0$. This leads to a contradiction if g is odd. If g is even, we have already seen that such curves exist. \square

Theorem 4.7. *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 either $\sigma = 0$ and g is even or $\sigma > 0$ is even and $g > \sigma$.*

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.

The case where $\sigma = 0$ was considered in Lemma 4.6, so we assume that $\sigma > 0$. In particular, we show that for all even $\sigma > 0$ and all $g > \sigma$ there is a curve of genus g and 2-rank σ 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

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

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.

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

$$y^2 + y = x^5 + x^3 + \sum_{i=1}^k \left(\frac{1}{(x-x_i)^{a_i}} + \frac{1}{(x-x_i-1)^{a_i}} \right)$$

In this case, the map defined by $\tau(x) = x + 1, \tau(y) = y + x^2$ will have the desired properties.

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 $y^2 + y = h(x)$ where $h(x)$ has only simple poles. If τ^2 is hyperelliptic then $\tau(x) = x + b$ for some b and $\tau(y) = y + f(x)$ for some function $f(x)$. Without loss of generality, we may assume that the poles of $h(x)$ consist of $\{\infty, \alpha_1, \alpha_1 + b, \dots, \alpha_k, \alpha_k + b\}$ so that $h(x) = ax + \sum a_i \left(\frac{1}{x-\alpha_i} + \frac{1}{x-\alpha_i-b} \right)$. However, the fact that τ is an automorphism of the curve implies that $(f(x))^2 + f(x) = h(x) + h(x+b)$ or in other words that $(f(x))^2 + f(x) = ax + a(x+b)$ for some a . In particular, this implies that $(f(x))^2 + f(x)$ is a constant, which is a contradiction as $\tau^2(y) = y + 1$. \square

5. Automorphism Groups of Hyperelliptic Curves of a Given 2-rank

This section will combine the results of the previous 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.

We recall the easy group theoretic property that if every non-identity element of a group has order two then the group must be abelian and thus isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$ for some n . This will be the case for the automorphism group of a curve X of genus g and 2-rank σ if $2g + 1 - \sigma$ and $\sigma(\sigma^2 - 1)$ share no common odd factors (in which case X will admit no automorphisms of odd order by Theorem 3.2) and if either σ is odd or if $\sigma = 0$ and g is odd or if X is ordinary (in which case X will admit no automorphisms of order 4 by Theorem 4.7). However, Theorem 4.2 gives us more specific conditions on when $(\mathbb{Z}/2\mathbb{Z})^n$ can occur in the automorphism group of a curve X for various choices of n . Corollary 1.1 follows, giving explicit conditions on the genus and 2-rank under which a hyperelliptic curve must not admit any extra automorphisms.

As the automorphism groups get larger, it is trickier in general to tell one from another, 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 the cover will be ramified at a single point which we may assume without loss of generality is ∞ . Theorem 3.2 implies that we can have extra automorphisms of odd order m if and only if $m|2g + 1$. Furthermore, if g is odd then these will be the only allowable extra automorphisms. In particular, for any $m|2g + 1$ the curve defined by the equation $y^2 + y = x^{2g+1} + x^m$ must be a curve of genus g and 2-rank zero with automorphism group precisely $\mathbb{Z}/2m\mathbb{Z}$. One can check that this curve will have automorphism group $\mathbb{Z}/2m\mathbb{Z}$ even in the event that g is even. However, if g is even there will be other curves which admit extra involutions as well as automorphisms of degree four. We note that the 2-rank zero case is the same case considered by Lehr and Matignon in [8] using different techniques.

If $\sigma = 1$ then we do not need to consider automorphisms of order four. By Theorem 3.2 there will be curves with an extra automorphism of odd order m for all $m|g$ and if g is even then this is the only possibility. In particular, if m is the largest odd number dividing g then the curve defined by the equation $y^2 + y = x^m + \frac{1}{x^{2g-m}}$ will have automorphism group precisely $\mathbb{Z}/2m\mathbb{Z}$ and for smaller odd divisors one can similarly construct curves with the desired automorphism group. If g is odd then it follows from Theorem 4.2 that there will be curves of genus g and 2-rank one with extra involutions. Such a 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 the order of each pole is g . One can now check that if there is an extra automorphism of odd order $m > 1$ then it 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 $\zeta \neq 1$. In this case we will get a nonabelian automorphism group.

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 [16] that there exist 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 3.2 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 4.7. 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.

6. 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 2.1 to prove the following:

Lemma 6.1. *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 the former case, X will be a hyperelliptic curve whose equation can be given by $y^2 = f(x^m)$. In the latter case, we get the following theorem.

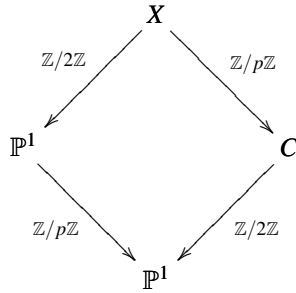
Theorem 6.2. *Let X be a hyperelliptic curve defined over an algebraically closed field of characteristic $p > 2$ which admits an extra automorphism of degree p . Let g be the genus of X and let σ be its p -rank. Then one of the following two cases occurs.*

- (1) $g \equiv \sigma \equiv p - 1 \pmod{p}$
- (2) $g \equiv \frac{p-1}{2}$ 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 .

12 *Darren Glass*

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 6.3. We note the similarity between Theorem 3.2 and Theorem 6.2. 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] S. Nakajima. p -ranks and automorphism groups of algebraic curves. *Trans. Amer. Math. Soc.*, 303(2):595–607, 1987.
- [10] 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.
- [11] H. Stichtenoth. Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkörpern. *Arch. Math. (Basel)*, 24:615–631, 1973.
- [12] H. Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer-Verlag, Berlin, 1993.
- [13] D. Subrao. The p -rank of Artin-Schreier curves. *Manuscripta Math.*, 16(2):169–193, 1975.
- [14] R. C. Valentini and M. L. Madan. A Hauptsatz of L. E. Dickson and Artin-Schreier extensions. *J. Reine Angew. Math.*, 318:156–177, 1980.
- [15] G. van der Geer and M. van der Vlugt. Fibre products of artin-schreier curves and generalized hamming weights of codes. *Journal of Combinatorial Theory, Series A*, 1995.
- [16] 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.