2012

Non-Genera of Curves With Automorphisms in Characteristic P

Darren B. Glass
Gettysburg College

Glass, Darren B. "Non-Genera of Curves With Automorphisms in Characteristic P." Computational Algebraic and Analytic Geometry, Contemporary Mathematics Vol. 572. Providence, RI: Amer. Math. Soc., 2012. 89-95.

Non-Genera of Curves With Automorphisms in Characteristic P

Abstract
We consider which integers g and r can occur respectively as the genus and p-rank of a curve defined over a field of odd characteristics p which admits an automorphism of degree p.

Keywords
algebraic curves, data processing, Riemann surfaces

Disciplines
Algebraic Geometry | Mathematics

Contemporary Mathematics
Volume **572**, 2012
http://dx.doi.org/10.1090/conm/572/11362

Non-genera of curves with automorphisms in characteristic p

Darren Glass

ABSTRACT. We consider which integers g and σ can occur respectively as the genus and p-rank of a curve defined over a field of odd characteristic p which admits an automorphism of degree p.

1. Introduction

This paper is intended to serve as a characteristic p analog to the paper by O'Sullivan and Weaver [**6**]. In that paper, the authors consider for which genera g there is a Riemann surface of genus g which admits an automorphism of order n for various choices of n. In this note, I consider the same question where we are instead working over an algebraically closed field of characteristic p and looking at curves admitting a $\mathbb{Z}/p\mathbb{Z}$-action. We determine which genera g can occur for such curves. Recall that the p-rank of a curve defined over a field k of characteristic p is the integer σ such that the cardinality of $\mathrm{Jac}(X)[p](k)$ is p^σ. It is well known that $0 \leq \sigma \leq g$ and in this note we establish conditions on pairs (g, σ) so that there exist curves of genus g and p-rank σ which admit a $\mathbb{Z}/p\mathbb{Z}$-action.

In the case $p = 2$, Zhu has shown in [**9**] that all pairs (g, σ) with $g \geq \sigma \geq 0$ occur as the genus and 2-rank of curves over $\mathbb{F}_2$, even for hyperelliptic curves with automorphism group exactly $\mathbb{Z}/2\mathbb{Z}$. In [**4**], the author considers curves admitting a $\mathbb{Z}/2m\mathbb{Z}$-action in characteristic 2 for all odd m. In light of these results, we restrict our attention to the situation where our field has odd characteristic in this note.

In particular, if we let $\langle a, b\rangle$ be the submonoid of $\mathbb{Z}$ generated by a and b (i.e. $\langle a, b\rangle = \{ax + by | x, y \in \mathbb{Z}_{\geq 0}\}$) then we show in Sections 2 and 3 the following necessary conditions for such a curve to exist.

THEOREM 1.1. *Let X be a curve of genus g and p-rank σ which admits a $\mathbb{Z}/p\mathbb{Z}$-action. Then we have the following conditions on g and σ.*

- *Either $g \in \langle p, \frac{p-1}{2}\rangle$ or $g \equiv 1 \pmod p$.*
- *Either $\sigma \in \langle p, p-1\rangle$ or $\sigma \equiv 1 \pmod p$*
- *$g - \sigma \in \langle p, \frac{p-1}{2}\rangle$*

These conditions are not sufficient for such a curve to exist; the difficulty comes because it is not possible to construct functions on arbitrary curves with arbitrary numbers of branch points and ramification degrees. Sections 2 and 3 prove that under additional hypotheses we can get sufficiency. One example of such a result

2010 *Mathematics Subject Classification.* Primary 14H37, 14H40; Secondary 11G20.

is Theorem 2.4 which gives precise conditions under which a curve of genus g with a $\mathbb{Z}/p\mathbb{Z}$-action exists. Another example is the following:

COROLLARY 1.2. *Let $\sigma \geq (p-1)(p+2)$. Then there exist curves of genus g and p-rank σ admitting a $\mathbb{Z}/p\mathbb{Z}$-action if and only if $g - \sigma \in \langle p, \frac{p-1}{2}\rangle$.*

We note that our results generalize the results in [**7**, Lemma 2.7], in which the authors considered the possible p-ranks of Artin-Schreier curves. Our results allow the quotient curve to have genus $g_Y > 0$, which allows for more possible values of g_X and σ. The main approach in our investigation will be to assume that X admits a $\mathbb{Z}/n\mathbb{Z}$-action with quotient Y, and consider the cover $X \to Y$. We then use the Riemann-Hurwitz formula to compare the genera of X and Y and the Deuring-Shafarevich formula to compare their p-ranks. We also use results about the Frobenius Problem (also known as the coin problem or the conductor problem), which asks what numbers are representable as nonnegative integral linear combinations of fixed integers. In particular, we recall the following theorem due to Sylvester [**8**], which is standard in any undergraduate number theory text:

THEOREM 1.3. *Let a and b be fixed coprime integers. Then any integer $d > ab - a - b$ can be expressed as a linear combination $d = ax + by$ where $x, y \in \mathbb{Z}_{\geq 0}$. Moreover, $ab-a-b \notin \langle a, b\rangle$ and exactly half of the integers between 1 and $ab-a-b+1$ are in $\langle a, b\rangle$.*

More generally, we will consider the sets $\langle a_1, \dots a_k\rangle$ of integers which can be expressed as the linear combination $a_1x_1 + \dots a_kx_k$ for nonnegative choices of x_i. While Sylvester's theorem gives us a description of these sets in the case where $k = 2$, the question becomes more difficult in the case where $k \geq 3$. In particular, while it is known that $\mathbb{Z}_{\geq 0} - \langle a_1, \dots a_k\rangle$ is a finite set, when $k \geq 3$ even finding the largest number in this set is NP-hard [**2**].

The author would like to thank Tony Weaver, Rachel Pries, and the referees for many valuable suggestions.

2. Non-genera for $\mathbb{Z}/p\mathbb{Z}$-actions

Let us begin by considering what genera occur as g_X for some cover $X \to Y$ whose degree is p when working over a field of odd characteristic p. We recall that a $\mathbb{Z}/p\mathbb{Z}$-cover $X \to Y$ is defined by an equation $T^p - T = F$ where F is a function on the curve Y. Moreover, if the function F has poles of order n_i all of which are relatively prime to p, then the Riemann-Hurwitz formula in characteristic p tells us that $g_X = pg_Y - p + 1 + \frac{p-1}{2}\sum(n_i + 1)$. Throughout this paper, we will define the ramification type of a function with m poles of orders n_i to be the m-tuple $(n_1, \dots, n_m)$. To illustrate our method, we begin by considering some examples.

EXAMPLE 2.1. *Let $p = 3$. The Riemann-Hurwitz formula implies that $g_X = 3g_Y - 2 + \sum(n_i + 1)$. Let us consider the case where $g_Y = 0$, and consider curves ramified at two points, so that $g_X = n_1 + n_2$. We note that the only restriction on the values of n_i is that they cannot be multiples of 3. In particular, one can obtain all values of $g_X \geq 2$ by setting either $n_1 = 1$ and $n_2 = g_X - 1$ or $n_1 = 2$ and $n_2 = g_X - 2$. Moreover, one can construct a curve with $g_X = 0$ (resp. 1) by looking at the cover $X \to Y$ ramified at a single point with ramification degree 1 (resp. 2). This implies that every g_X occurs as the genus of an Artin-Schreier curve in characteristic 3 ramified in at most two points.*

EXAMPLE 2.2. *Let $p = 5$. In this case, the Riemann-Hurwitz formula implies that $g_X = 5g_Y - 4 + 2\sum(n_i + 1)$. We again set $g_Y = 0$ and allow our cover to have two ramification points, so that $g_X = 2(n_1 + n_2)$. Moreover, all even numbers $g_X \geq 4$ can occur in this case, again by choosing $n_1 = 1$ or 2. Furthermore, an Artin-Schreier curve of genus 0 (resp. 2) can be constructed with a single ramification point.*

While parity restrictions mean that we are unable to construct covers over $\mathbb{P}^1$ of odd genus in this case, we may be able to construct curves X of odd genus that are covers of elliptic curves. The situation here is slightly more complicated, however, as to do so one must construct functions on curves of genus 1 with prescribed ramification divisors. For example, there are no functions on elliptic curves which have a single pole of order one. As we will see below, however, the restrictions are not as severe as they may initially seem.

We note the following result is true regardless of the characteristic:

LEMMA 2.3. *Let Y be a curve of genus 0. Then for any nonnegative integer R except $R = 1$ there exists a function F on Y with poles of order n_i so that $p \nmid n_i$ for all i and $\sum(n_i + 1) = R$.*

Let Y be a hyperelliptic curve of genus $g_Y > 0$. Then for any nonnegative integer $R \neq 1, 2$ there exists a function F on Y with poles of order n_i so that $p \nmid n_i$ for all i and $\sum(n_i + 1) = R$. No such function exists for $R = 1$ or 2

PROOF. On any curve Y there exist constant functions. These have no poles and therefore give the existence of functions where $\sum(n_i + 1) = 0$.

On a curve of genus zero, there exists a function with a single pole of order one, and therefore the appropriate power of this function will have ramification type $(R-1)$ as long as $R \not\equiv 1 \pmod{p}$. If $R \equiv 1 \bmod p$ we can construct a function that has one pole of order $R - 3$ (which will not be a multiple of p as $p > 2$) and a second pole of order 1. These two examples prove the first part of the lemma.

To prove the second part of the lemma, we note that hyperelliptic curves automatically come equipped with functions that have ramification type (2) and $(1, 1)$ and in particular there are many of the latter type of function. It is therefore possible to consider linear combinations of these functions that will have ramification type $(2k), (k, k), (2k, 1, 1)$ and $(k, k, 1, 1)$ for all $k > 0$ and $p \nmid k$. In particular, this allows us to get values of R of the form $2k + 1, 2k + 2, 2k + 5$ and $2k + 6$ for any $p \nmid k$. Every positive integer other than 1 and 2 takes one of these forms. Note that $R = 1$ is impossible as, if a function has a pole at a point then that order must be at least one and vice versa. Moreover, the only way to obtain $R = 2$ would be to have a single simple pole, which is impossible on curves of genus $g \geq 1$ (See, for example, [**3**, §8.2, Prop 4]). $\square$

Applying this lemma to our previous example, we are able to construct curves of all odd genera other than $g_X = 3$ or 5 as $\mathbb{Z}/5\mathbb{Z}$-covers of curves of genus one. More generally, we note that computing the set of values g_X that can occur has now been reduced to something that is very similar to the two-dimensional Frobenius Problem connected to the coprime pair of numbers p and $\frac{p-1}{2}$. In particular, we can apply Theorem 1.3 to learn about the nonnegative linear combinations of p and $\frac{p-1}{2}$ and then remove those entries where $b = 0$ and $a > 0$ (all of which are multiples of p) and add in the entries where $b = -2$ (all of which are congruent to one mod p).

THEOREM 2.4. *Define the set*

$$G = \left(\langle p, \frac{p-1}{2} \rangle - \left\{ kp | 0 \leq k < \frac{p-1}{2} \right\} \right) \cup \{kp+1 | k \in \mathbb{Z}_{\geq 0}\}.$$

Then there exists a curve of genus g defined over an algebraically closed field of characteristic p and admitting a $\mathbb{Z}/p\mathbb{Z}$-action if and only if $g \in G$. Moreover, there are exactly $\frac{p^2-4p+3}{4}$ nonnegative integers not in G, the largest of which is $\frac{p^2-3p}{2}$.

PROOF. In order to construct a curve X of genus g_X which admits a $\mathbb{Z}/p\mathbb{Z}$-action, it suffices to construct a curve Y of genus g_Y and a function on Y so that $\sum(n_i+1) = R$ where $g_X = pg_Y - p + 1 + \frac{p-1}{2}R$. Lemma 2.3 tells us that for most choices of nonnegative integers g_Y and R we can do this. By also allowing the case of unramified covers, it follows that g_X can be expressed as a linear combination $ap + b\frac{p-1}{2}$ where $a = g_Y$ is a nonnegative integer and $b = \sum(n_i+1) - 2$ is either equal to -2 or is a positive integer. Additionally, if $a = 0$ then b is allowed to be 0 as well.

Theorem 1.3 tells us that $\langle p, \frac{p-1}{2} \rangle$ consists of all but $\frac{p^2-4p+3}{4}$ nonnegative integers, and that the largest integer not contained in this set is $\frac{p^2-4p+1}{2}$. We must eliminate all of the genera that arise in the Frobenius problem with $b = 0$ and $a > 0$. In particular, one cannot have curves whose genus is a multiple of p less than $p \cdot \frac{p-1}{2}$ admitting a $\mathbb{Z}/p\mathbb{Z}$-action, so we 'lose' $\frac{p-3}{2}$ possible genera. Moreover, the largest such number is $p \cdot \frac{p-3}{2}$, which is larger than the largest number not lying in $\langle p, \frac{p-1}{2} \rangle$.

On the other hand, if $b = -2$ then we have the equation $g = (a-1)p + 1$ where $a \in \mathbb{N}$. Because we are only interested in the case where $g \geq 0$, this tells us that $g \equiv 1 \mod p$. and that any such genus can be obtained as an unramified cover. We also note that if $g \equiv 1 \mod p$ and $g < \frac{p^2-4p+1}{2}$ then g cannot be representable as a nonnegative linear combination of p and $\frac{p-1}{2}$. In particular, if $g = ap + b\frac{p-1}{2}$ then $b \equiv -2 \mod p$ and therefore $b \geq p-2$. But this implies that $g \geq \frac{(p-2)(p-1)}{2} > \frac{p^2-4p+1}{2}$. Therefore, all of the $\frac{p-3}{2}$ genera which are congruent to one are in fact new examples and exactly offset those genera lost in the previous paragraph. This proves the theorem. $\square$

We conclude this section by listing the values of g_X that do not occur as genera of a curve admitting a $\mathbb{Z}/p\mathbb{Z}$-action for some small values of p.

p	non-genera
3	none
5	$3, 5$
7	$2, 4, 5, 7, 11, 14$
11	$2, 3, 4, 6, 7, 8, 9, 11, 13, 14, 17, 18, 19, 22, 24, 28, 29, 33, 39, 44$

3. p-ranks

In this section, we consider the p-ranks which can occur for curves of various genera that are defined over an algebraically closed field of characteristic p and admit a $\mathbb{Z}/p\mathbb{Z}$-action. Our main tool will be the following fact, which follows from the Deuring-Shafarevich formula [**1**]:

LEMMA 3.1. *Let $X \to Y$ be a $\mathbb{Z}/p\mathbb{Z}$-cover of curves ramified at n points, where X has p-rank σ_X and Y has p-rank σ_Y. The p-ranks are related by the formula $\sigma_X = p\sigma_Y + (p-1)(n-1)$.*

It follows from the lemma that if X is a curve admitting a $\mathbb{Z}/p\mathbb{Z}$-action ramified in at least one point then its p-rank σ_X is representable as a nonnegative linear combination of p and $p-1$ and if the action is unramified then σ_X is congruent to 1 mod p. Moreover, any such p-rank can be obtained by choosing an appropriate Y and n. The values of σ that do not satisfy these conditions are given by

$$2, 3, \dots, p-2, p+2, \dots, 2p-3, 2p+2, \dots, 3p-4, \dots, (p-4)p+2$$

and in particular, there are $\frac{p^2-p-4}{2}$ non-p-ranks, as described by the following theorem.

THEOREM 3.2. *Let $\sigma = kp - s$ where $0 \leq s < p$. Then there are no curves of p-rank σ which admit a $\mathbb{Z}/p\mathbb{Z}$-action if $1 \leq k < s \leq p-2$.*

All other values of σ occur as the p-rank of some curve admitting a $\mathbb{Z}/p\mathbb{Z}$-action, but not all possible p-ranks occur alongside all possible genera, and the next theorem gives a condition on which pairs (g, σ) can simultaneously occur as the genus and the p-rank of a curve admitting a $\mathbb{Z}/p\mathbb{Z}$-action.

THEOREM 3.3. *Let X be a curve of genus g_X and p-rank σ_X which admits a $\mathbb{Z}/p\mathbb{Z}$-action. Then $g_X - \sigma_X \in \langle p, \frac{p-1}{2} \rangle$.*

PROOF. Let X be a curve of genus g_X and p-rank σ_X which admits a $\mathbb{Z}/p\mathbb{Z}$-action ramified at n points and let Y be the quotient of the curve X by the $\mathbb{Z}/p\mathbb{Z}$-action. One can compute from the Riemann-Hurwitz formula that $g_X = pg_Y - (p-1) + \frac{p-1}{2}R$ where R is the degree of the ramification divisor and in particular must be at least $2n$. Setting $a = g_Y - \sigma_Y \geq 0$ and $b = R - 2n \geq 0$, we compute:

$$\begin{aligned}
g_X &= pg_Y - (p-1) + \frac{p-1}{2}R \\
&= p(g_Y - \sigma_Y) + p\sigma_Y - (p-1) + \frac{p-1}{2}(R-2n) + \frac{p-1}{2}(2n) \\
&= pa + \sigma_X - (n-1)(p-1) - (p-1) + \frac{p-1}{2}b + (p-1)n \\
&= pa + \frac{p-1}{2}b + \sigma_X \\
&\in \langle p, \frac{p-1}{2} \rangle + \sigma_X
\end{aligned}$$

□

In order to prove conditions which are sufficient in addition to being necessary, we need to show when there exists a function that has prescribed choices of R and n. The following lemma will give some existence results in this direction.

LEMMA 3.4. *Let Y be a hyperelliptic curve and let R and m be integers such that $R \geq 2m > 0$ and $R \equiv m \pmod 2$. Additionally, if $m = 1$ assume that $R \not\equiv 1 \pmod p$ and if $m = 2$ assume that $R \not\equiv 2 \pmod p$. Then there exists a function F on Y which has m poles of orders $n_1, \dots n_m$ so that $p \nmid n_i$ for all i and $\sum(n_i + 1) = R$.*

PROOF. As in the proof of Lemma 2.3 we begin by noting that hyperelliptic curves admit a function with a single pole of order 2 and they admit many functions that admit two simple poles. In particular, we can look at combinations of such functions to obtain functions with m poles that have the following ramification types with the associated conditions on m and k

Ram. Type	$\sum(n_i+1)$	m	k
$(k,k,1,\ldots,1)$	$2k+2m-2$	$m \geq 2$ & even	$p \nmid k$
$(k-1,k-1,2,2,1,\ldots,1)$	$2k+2m-2$	$m \geq 4$ & even	$p \nmid (k-1)$
$(2k,1,\ldots,1)$	$2k+2m-1$	$m \geq 1$ & odd	$p \nmid k$
$(2k-2,2,2,1,\ldots,1)$	$2k+2m-1$	$m \geq 3$ & odd	$p \nmid (k-1)$

This proves the lemma. □

THEOREM 3.5. *Let $\sigma = rp + s(p-1)$ with $r \geq 0$ and $s \geq 2$. Let $\epsilon = 1$ if s is even and $\epsilon = 0$ if s is odd. If $g - \sigma - \epsilon\frac{p-1}{2} \in \langle p, p-1\rangle$ then there exists a curve of genus g and p-rank σ admitting a $\mathbb{Z}/p\mathbb{Z}$-action.*

We note that if σ is sufficiently large then one can express it in the desired form for either even or odd choices of s. Explicitly, if $r \geq p-1$ then $rp + s(p-1) = (r-p+1)p + (s+p)(p-1)$ and $s+p$ will have opposite parity as s. Corollary 1.2 is an immediate consequence of Theorem 3.5.

PROOF. By the hypotheses, we can write $g_X = ap + b(p-1) + rp + s(p-1) + \epsilon\frac{p-1}{2}$ for some $a, b \geq 0$. We wish to construct a curve with genus g_X and p-rank σ_X which has a $\mathbb{Z}/p\mathbb{Z}$-action. In order to do this, we define $\sigma_Y = r$ and $g_Y = a + r$. It follows from **[5]** that there exist hyperelliptic curves of genus g_Y and p-rank σ_Y; let Y be one such curve.

It follows from Lemma 3.4 that as long as $s \geq 2$ there exists a function F on Y which is ramified at $s+1$ points with ramification degree $n_1, \ldots, n_{s+1}$ so that $\sum(n_i+1) = 2s + 2b + 2 + \epsilon$. We let X be the curve defined by the cover $T^p - T = F$. It follows from the Riemann-Hurwitz and Deuring-Shafarevich formulae that:

$$\begin{aligned}
\mathrm{genus}(X) &= pg_Y - (p-1) + \frac{p-1}{2}\left(\sum(n_i+1)\right) \\
&= ap + rp - p + 1 + \frac{p-1}{2}(2s + 2b + 2 + \epsilon) \\
&= ap + b(p-1) + rp + s(p-1) + \epsilon\frac{p-1}{2} \\
&= g_X
\end{aligned}$$

and

$$\begin{aligned}
p\text{-rank of } X &= p\sigma_y + (p-1)(n-1) \\
&= pr + (p-1)s \\
&= \sigma_X
\end{aligned}$$

as desired. □

We note that allowing $s = 0$ and $s = 1$ would allow us to choose smaller values of σ_X and therefore somewhat increase our range of allowable p-ranks. However, this would add a congruence restriction on the ramification divisor and therefore on the possible genera. We leave the details to the reader.

Throughout this section, we have assumed that our base field is algebraically closed. However, we note that the construction we give proving existence will work over any field K of characteristic p so that there exists a hyperelliptic curve of genus g_Y and p-rank σ_Y with an appropriate number of points defined over K. In general, the question about the minimal field over which such a curve will exist is open – in particular, it is not even known whether curves of general genus and p-rank exist over $\mathbb{F}_p$, even without a restriction on the number of rational points.

References

1. Richard M. Crew, *Etale p-covers in characteristic p*, Compositio Math. **52** (1984), no. 1, 31–45. MR742696 (85f:14011)
2. Frank Curtis, *On formulas for the Frobenius number of a numerical semigroup*, Math. Scand. **67** (1990), no. 2, 190–192. MR1096454 (92e:11019)
3. William Fulton, *Algebraic curves. An introduction to algebraic geometry*, W. A. Benjamin, Inc., New York-Amsterdam, 1969, Notes written with the collaboration of Richard Weiss, Mathematics Lecture Notes Series. MR0313252 (47:1807)
4. Darren Glass, *The 2-ranks of hyperelliptic curves with extra automorphisms*, Int. J. Number Theory **5** (2009), no. 5, 897–910. MR2553515 (2010h:11100)
5. Darren Glass and Rachel Pries, *Hyperelliptic curves with prescribed p-torsion*, Manuscripta Math. **117** (2005), no. 3, 299–317. MR2154252 (2006e:14039)
6. Cormac O'Sullivan and Anthony Weaver, *A Diophantine Frobenius problem related to Riemann surfaces*, Glasg. Math. J. **53** (2011), no. 3, 501–522. MR2822795
7. Rachel Pries and Hui June Zhu, *The p-rank stratification of Artin-Schreier curves*, Annales de l'Institut Fourier, to appear.
8. J. J. Sylvester, *Question 7382*, Mathematical Questions from the Educational Times **41** (1884).
9. Hui June Zhu, *Hyperelliptic curves over $\mathbb{F}_2$ of every 2-rank without extra automorphisms*, Proc. Amer. Math. Soc. **134** (2006), no. 2, 323–331. MR2175998 (2006h:11074)

Department of Mathematics, Gettysburg College, 300 N. Washington Street, Gettysburg, Pennsylvania 17325

E-mail address: dglass@gettysburg.edu