

Darren Glass: Description of Current Research Interests Spring 2008

My research interests are generally in the areas of algebraic geometry, number theory, and Galois theory. My dissertation and some of the research at that time focussed on profinite Galois groups ([2]) and ε -constants associated to arithmetic schemes ([5], [6]), and I have continued this work with a more recent paper on the De Rham cohomology of elliptic curves ([9]). However, most of my recent projects have investigated the automorphism groups of algebraic curves defined over fields of characteristic p , and in particular the relationship between the automorphism group of a given curve and the number of rational points on such curves. Questions about these two invariants as well as the relationship between them have implications throughout arithmetic geometry, cryptography, and coding theory. This note is an attempt to summarize and explain some of the work I have done on these questions as well as to pose some questions which I hope to consider in the future.

Determining what groups act as a group of automorphisms of an algebraic curve is an old problem of algebraic geometry and group theory. There is a vast literature on automorphism groups of algebraic curves, beginning in the 19th century with Schwartz, Klein, Hurwitz, Wiman and others. Determining the list of groups that occur as full automorphism groups of algebraic curves for a fixed genus g seems to be a difficult problem. In characteristic zero, Breuer determined methods to compute all possible signatures of a group acting on curves of a given genus if one has sufficient computing power. Magaard, Shaska, Shpectorov and Völklein used Breuer's results to design an algorithm which determines the full automorphism groups of curves; see [16] for full references and details on this topic as well as the complete results for $g \leq 6$. Their work fully solves the problem in characteristic zero. The case of algebraic curves defined over a field of positive characteristic is much different due to the presence of wild ramification. In particular, the Riemann existence theorem is no longer valid and the methods of [16] can not be used, leading to the following question.

Question 1 *Given a field k of characteristic $p > 0$ and a fixed integer g , what are the possible automorphism groups of curves of genus g defined over k ? Which groups occur if we restrict our attention to hyperelliptic curves?*

This question has been fully answered in the case where $g = 2$ (see [18] among others) and the case of $g = 3$ is considered in an unpublished PhD thesis by Henn. An ongoing collaboration of mine with Tony Shaska [13] has attempted to streamline (and translate) Henn's results and also to classify all possible automorphism groups of curves of genus four. A theorem of Blichfeld implies that the genus g curve lifts to characteristic 0 for $p > 2g + 1$ and in this case we can use the methods described in [16] can be used to determine the possible automorphism groups. The case where $p \leq 2g + 1$ must be handled separately, and Shaska and I have approached this problem by first analyzing the cyclic covers and classifying which automorphism groups can occur for $\mathbb{Z}/p\mathbb{Z}$ -covers before moving on to the general case, where one can work explicitly with different covers. We anticipate having a preprint of this work completed by the end of the summer in 2008.

One result which holds only in characteristic zero is Hurwitz's theorem that curves of genus $g \geq 2$ have at most $84(g-1)$ automorphisms. When the characteristic of the base field is $p > 0$ this bound does not carry over, but Stichtenoth has proven a different bound that in general the number of automorphisms of an algebraic curve of genus g will be strictly less than $16g^4$, with a small, completely described set of exceptions. For example, the curve defined by $y^{p^n} + y = x^{p^{n+1}}$ has genus $g = \frac{1}{2}p^n(p^n - 1)$ but admits $p^{3n}(p^{3n} + 1)(p^{2n} - 1)$ automorphisms, so $|G|$ is larger than $16g^4$. This family of curves has a number of other interesting properties, and in some recent work with David Joyner and Amy Ksir appearing in [8] we have attempted to analyze some of the features of these curves. More specifically, we look at the curve $y^2 = x^p - x$ and worked out an explicit basis for the Riemann-Roch space of this curve defined over \mathbb{F}_p . In particular, one can show that the automorphism group G of this curve is isomorphic to $SL_2(p)$, and that the G -invariant divisors on the curve are all multiples of a single divisor D . From there, we prove the following result about the basis of the Riemann-Roch space $L(rD)$:

Theorem 1 *Define the vector spaces $A_i = \text{Span}\left\{\frac{x^j}{(x^p-x)^i} \mid 0 \leq j \leq i(p+1)\right\}$ and $B_i = \text{Span}\left\{\frac{yx^j}{(x^p-x)^i} \mid 0 \leq j \leq i(p+1) - \frac{p+1}{2}\right\}$ with the convention that $A_0 = \mathbf{1}$ and $B_0 = \{0\}$. Then for all $r \geq 1$ we have $L(rD) = A_{\lfloor \frac{r}{2} \rfloor} \oplus B_{\lceil \frac{r}{2} \rceil}$.*

We also prove a series of similar results about the Riemann-Roch space of this curve when it is defined over other finite fields of characteristic p , as well as other related curves. The eventual goal of this research project is to understand the answer to the following question, which would have interesting uses in coding theory:

Question 2 *What are explicit sets of basis elements for the Riemann-Roch spaces of other 'large' curves (ie curves X whose automorphism group G satisfies $|G| > |X(F)|$) and therefore every point of X is ramified in the quotient map $X \rightarrow X/G$)*

When investigating abelian varieties defined over a field of characteristic p , it is natural to look at the group schemes which arise as the p -torsion of Jacobians of such varieties. In the case of elliptic curves, there are only two possible group schemes which arise, corresponding to ordinary and supersingular elliptic curves. For curves of higher genus, the group schemes get more complicated and there are many more possible group schemes which can arise. In order to get a handle on the problem, one often wishes to study the invariants related to these group schemes such as their p -rank or a -number. The p -rank of a curve X (or, more precisely, the p -rank of its Jacobian) can be defined as $\dim_{\mathbb{F}_p} \text{Hom}(\mu_p, \text{Jac}(X))$ where μ_p is the kernel of Frobenius on \mathbb{G}_m . In particular, curves of p -rank σ will have precisely p^σ distinct p -torsion points on their Jacobian. The p -rank is quite well-understood and Oort [17] and others have used it to define stratifications of the moduli space \mathcal{A}_g of principally polarized abelian varieties of dimension g . There is a deep interest in understanding how the Torelli locus consisting of abelian varieties which are Jacobians of curves intersects such strata in \mathcal{A}_g . Throughout this note, we will denote the space of curves of genus g whose p -rank is at most f by $V_{g,f}$. Faber and van der Geer show in [4] that $V_{g,f}$ is nonempty for all

$0 \leq f \leq g$ and in particular that there exist smooth curves of every genus g and every p -rank.

Many arithmetic geometers believe that curves which admit many automorphisms should have small p -rank. The idea behind this philosophy is that any automorphism of a curve will permute the p -torsion points on the curve, and this should lead to a restriction on the possible number of these points. This idea has never been precisely put into the form of a conjecture or theorem, but several attempts have been made to investigate the relationship between automorphism groups and p -ranks, leading to the following natural refinement of Question 1:

Question 3 *For a given field k of positive characteristic p and a given automorphism group G , classify the possible pairs (g, f) so that there exist (hyperelliptic) curves defined over k of genus g and p -rank f .*

The simplest example of curves admitting nontrivial automorphisms come from \mathcal{H}_g , the locus of hyperelliptic curves of a given genus. Rachel Pries and I prove the following theorem in [10], generalizing the result of Faber and van der Geer to the case of hyperelliptic curves:

Theorem 2 *For all $0 \leq f \leq g$, the locus $V_{g,f} \cap \mathcal{H}_g$ is non-empty of dimension $g - 1 + f$. In particular, there exists a smooth hyperelliptic curve of genus g and p -rank f .*

Another invariant of Jacobians of curves in characteristic p is given by the a -number of such a curve. The a -number is given by $\dim_k \text{Hom}(\alpha_p, \text{Jac}(X))$, where $\alpha_p \cong \text{Spec}(k[x]/x^p)$ is the kernel of Frobenius on \mathbb{G}_a . In [10], we also prove results about the existence of hyperelliptic curves of a given genus and a -number. One example of such a result is the following:

Theorem 3 *If $g \geq 2$ and $p \geq 5$ then there exists a $(g - 2)$ -dimensional family of smooth hyperelliptic curves of genus g all of whose fibres have a -number equal to 2. Similarly, if $g \geq 5$ and $p \geq 7$ then there exists a $(g - 5)/2$ -dimensional family of smooth hyperelliptic curves of genus g and a -number at least 3.*

The method used to prove these results involves looking at curves which are $(\mathbb{Z}/2\mathbb{Z})^2$ -covers of \mathbb{P}^1 and using results of Kani and Rosen from [15] to relate the invariants of these curves to the invariants of their (hyperelliptic) $\mathbb{Z}/2\mathbb{Z}$ -quotients. While we were able to answer several questions about the p -ranks and a -numbers of curves using these methods, this work raised several more questions that could be tackled using our methods if we had better control over the invariants for hyperelliptic curves. In [12], we discuss some specific open questions, such as the following, and discuss the implications of their answers:

Question 4 *Given an arbitrary hyperelliptic cover $C \rightarrow \mathbb{P}^1$, is it possible to deform C to an ordinary hyperelliptic curve (that is, one with equal p -rank and genus) by moving only one of its branch points?*

This research led us to consider more generally the moduli space of G -covers of \mathbb{P}^1 , where $G = (\mathbb{Z}/2\mathbb{Z})^n$. We denote the moduli space of all such smooth curves of genus g as $\mathcal{H}_{g,n}$ and we are able to characterize such curves in the following way:

Theorem 4 *A cover $f : X \rightarrow \mathbb{P}^1$ corresponds to a point of $\mathcal{H}_{g,n}$ if and only if X has genus g and $f : X \rightarrow \mathbb{P}^1$ is isomorphic to the normalized fibre product over \mathbb{P}^1 of n smooth hyperelliptic covers $C_i \rightarrow \mathbb{P}^1$ whose branch loci B_i satisfy a strong disjointness condition.*

This characterization is made more precise in [11], where we also prove the following results about the components of $\mathcal{H}_{g,n}$:

Theorem 5 *If $g \equiv 1 \pmod{2^{n-2}}$ then the Hurwitz space $\mathcal{H}_{g,n}$ is the union of closed smooth connected schemes $\mathcal{H}_{g,n,\vec{g}}$ each of which is of dimension $\frac{g+2^n-1}{2^{n-2}} - 3$. These schemes are indexed by tuples $\vec{g} = (g_1, \dots, g_N)$ where $N = 2^n - 1$ with $g_i \in \mathbb{N}$ and $\sum_{i=1}^N g_i = g$. These schemes will be nonempty as long as the g_i satisfy certain restrictions coming from the Riemann-Hurwitz formula. If g is not congruent to $1 \pmod{2^{n-2}}$ then $\mathcal{H}_{g,n}$ is empty.*

Finally, we are able to prove the following result about the disconnectedness of $\mathcal{H}_{g,n}$:

Theorem 6 *For any fixed n and g there is a unique irreducible component \mathcal{H}_{g,n,p_0} corresponding to those curves in $\mathcal{H}_{g,n}$ which are hyperelliptic. For sufficiently large g , \mathcal{H}_{g,n,p_0} does not intersect any other components of $\mathcal{H}_{g,n}$. In particular, $\mathcal{H}_{g,n}$ is not connected.*

This work led to the following question, which can be answered in the affirmative in the case where $j = 2$ but is much harder for $j > 2$. Work of Karl Rubin and others has shown that affirmative answers to this question for large j has implications related to the Parity Conjecture as well as the Birch-Swinnerton-Dyer Conjecture.

Question 5 *Is it possible to construct a curve $X \in \mathcal{H}_{g,n}$ such that X is the fibre product of n hyperelliptic curves, j of which are isogenous (or, better yet, isomorphic) elliptic curves? Is it possible to construct such an $X \in \mathcal{H}_{g,n,p_0}$? (ie with X itself hyperelliptic)*

One also wonders whether the methods used in [11] could be extended to consider other Hurwitz spaces. I have done preliminary work on looking at the moduli space of dihedral covers of the projective line as well as $(\mathbb{Z}/p\mathbb{Z})^n$ -covers of \mathbb{P}^1 and while some of the technical issues get increasingly complicated, I am optimistic that this approach will continue to lead to fruitful research projects.

Once again, due to the presence of wild ramification, the methods which Pries and I developed were unable to handle the case where the ground field had characteristic two. However, different methods which build off of results of van der Geer and van der Vlugt in [19] have allowed me to move some of my attention to this case in more recent work. In [14], I look at Klein-four covers of the projective line over an algebraically closed field of characteristic two. In this paper, I show that there exist curves in $\mathcal{H}_{g,2}$ of genus g and 2-rank f defined over \mathbb{F}_4 for all $0 \leq f \leq g$ except for $f = g - 1$ or, in the case where g is even, $f = 1$. More precisely, if we define the *type* of a $\mathbb{Z}/2\mathbb{Z}$ -cover $X \rightarrow \mathbb{P}^1$ in $\mathcal{H}_{g,2}$ to be the unordered triple $\mathfrak{p} = \{g_1, g_2, g_3\}$ corresponding to the genera of the three $\mathbb{Z}/2\mathbb{Z}$ quotients of X then we can prove the following theorem (see [14] for relevant definitions):

Theorem 7 *There exist curves of 2-rank σ in $\mathcal{H}_{g,2}$ for all $0 \leq \sigma \leq g$ and any type \mathfrak{p} except in the following cases:*

- i. $\sigma = 0$, $\mathfrak{p} \neq \{g_1, g_1, g_3\}$ with $g_3 \leq g_1$.
- ii. $\sigma = 1$, $\frac{g+1}{2} \notin \mathfrak{p}$.
- iii. $\sigma = 2$, $\mathfrak{p} = \{g_1, g_1, g_1\}$.
- iv. $\sigma = g - 1$.
- v. $\sigma \not\equiv g \pmod{2}$, either $\frac{g}{2}$ or $\frac{g+1}{2}$ in \mathfrak{p} .

In some unpublished work, I further look at the case of $\mathcal{H}_{g,n}$ for $n \geq 3$ and I am able to place restrictions on the 2-ranks of curves that are $(\mathbb{Z}/2\mathbb{Z})^n$ -covers of the projective line in this situation. One immediate consequence of Theorem 7 is the following:

Theorem 8 *There are hyperelliptic curves of genus g and 2-rank σ which contain an additional involution in their automorphism group if and only if $g \equiv \sigma \pmod{2}$.*

We note that this result is complementary to a result of Zhu. In [20], she shows that there are hyperelliptic curves of every 2-rank that have automorphism group precisely $\mathbb{Z}/2\mathbb{Z}$. Theorem 8 shows that having an extra (ie nonhyperelliptic) automorphism of order two places a strict restriction on the relationship between the genus and 2-rank of a curve. I continued to explore this complementary question in [7], in which I show that having ‘extra’ (ie nonhyperelliptic) automorphisms puts restrictions on the relationships between the genus and the 2-rank. One example of the type of result shown in [7] is the following theorem:

Theorem 9 *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 $g \equiv 0, 4, 6, 10, 16, 18, 24, 28 \pmod{30}$.

The results in [7] further show some of the possible automorphism groups of hyperelliptic curves of a given genus and 2-rank in characteristic two. Most of these results are nonconstructive and as such do not give insight into the fields of definition of the curves. However, Theorems 7 and 9 do start to give answers to Question 3. In a similar vein, I have been able to prove results about the ‘extra automorphisms’ that Artin-Schreier curves (that is, curves which are $\mathbb{Z}/p\mathbb{Z}$ -covers of \mathbb{P}^1 defined over a field of characteristic p) may have and the restrictions which these automorphisms place on the genus and p -ranks of such curves. These theorems are essentially the analogue of Theorem 9 in the case where $p > 2$, although some further subtleties appear.

In addition to considering these questions which I view as complementary to Zhu’s results in [20], Jeff Achter and Rachel Pries and I have been able to prove a result which strengthens Zhu’s result in certain ways. In particular, we are able to show in [1] that over an algebraically closed field of any positive characteristic that the generic hyperelliptic curve of a given p -rank has automorphism group exactly $\mathbb{Z}/2\mathbb{Z}$. In particular, we prove the following:

Theorem 10 *Let k be an algebraically closed field of characteristic $p > 0$. Furthermore, suppose $g \geq 3$ and $0 \leq f \leq g$.*

- (i) *There exists a smooth projective k -curve C of genus g and p -rank f with $\text{Aut}(C) = \{1\}$.*
- (ii) *There exists a smooth projective hyperelliptic k -curve D of genus g and p -rank f with $\text{Aut}(D) \simeq \mathbb{Z}/2$.*

Throughout this note, I have mentioned several open questions which I have thought about and will continue to work on. I will end by briefly discussing some of the other problems in this area that I plan to work on in the near future.

Question 6 *What are the possible a -numbers for $\mathbb{Z}/p\mathbb{Z}$ -covers of the projective line in characteristic p which have a given p -rank?*

Work of Elkin and Pries in [3] has shown among other things that if one looks at hyperelliptic curves in characteristic two which have 2-rank equal to zero, they all must have a -number equal to $\frac{g}{2}$. Some further work that I have done with them suggests that more generally there is a small range of possible a -numbers for $\mathbb{Z}/p\mathbb{Z}$ -covers of \mathbb{P}^1 which have p -rank zero. We hope to continue this research and prove results answering Question 6.

Question 7 *Is it possible to specify the fields of definition of the curves constructed in the above Theorems?*

Most of the proofs of the results discussed in this note are geometric and non-constructive. As such, they give no information about the field of definition of the curves of a given genus and p -rank with trivial automorphism group. However, for many applications in cryptography and elsewhere, it is important to know if the curves can be defined over \mathbb{F}_p or over a small extension of \mathbb{F}_p .

Finally, I would be very interested in the answer to the following generalizations of Theorem 10:

Question 8 Does the generic curve in $\mathcal{H}_{g,2} \cap V_{g,f}$ have automorphism group exactly $(\mathbb{Z}/2\mathbb{Z})^2$? More generally, for $n \geq 2$ does the generic curve in $\mathcal{H}_{g,n} \cap V_{g,f}$ have automorphism group exactly $(\mathbb{Z}/2\mathbb{Z})^n$?

Question 9 Does the generic Artin-Schreier curve of a given genus and p -rank have automorphism group exactly $\mathbb{Z}/p\mathbb{Z}$?

References

- [1] J. Achter, D. Glass, and R. Pries. The automorphism group of a generic curve with given p -rank. *Michigan Journal of Mathematics*, accepted for publication.
- [2] T. Chinburg and D. Glass. Embedding problems and finite quotients. *Pacific J. Math.*, 205(1):31–41, 2002.
- [3] Arsen Elkin and Rachel Pries. Hyperelliptic curves with a -number 1 in small characteristic. *Albanian J. Math.*, 1(4):245–252, 2007.
- [4] C. Faber and G. van der Geer. Complete subvarieties of moduli spaces and the Prym map. *J. Reine Angew. Math.*, 573:117–137, 2004.
- [5] D. Glass. Epsilon constants and orthogonal representations. *Compos. Math.*, 140(5):1135–1148, 2004.
- [6] D. Glass. Brauer group invariants associated to orthogonal epsilon-constants. *Bull. London Math. Soc.*, 37(2):172–178, 2005.
- [7] D. Glass. The 2-ranks of hyperelliptic curves with extra automorphisms. *International Journal of Number Theory*, accepted for publication.
- [8] D. Glass, D. Joyner, and A. Ksir. Basis of riemann-roch g -modules for $y^2 = x^p - x$ over $gf(p)$. in preparation.
- [9] D. Glass and S. Kwon. Galois structure of de rham cohomology. *Journal of Number Theory*, accepted for publication.
- [10] D. Glass and R. Pries. Hyperelliptic curves with prescribed p -torsion. *Manuscripta Math.*, 117(3):299–317, 2005.
- [11] 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.
- [12] D. Glass and R. Pries. Questions on p -torsion of hyperelliptic curves. *Rend. Sem. Mat. Univ. Padova*, 113, 2005.
- [13] D. Glass and T. Shaska. Automorphism groups of algebraic curves of genus 3 and 4 defined over fields of positive characteristic. in preparation.
- [14] Darren Glass. Klein-four covers of the projective line in characteristic two. *Albanian J. Math.*, 1(1):3–11 (electronic), 2007.
- [15] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284(2):307–327, 1989.
- [16] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein. The locus of curves with prescribed automorphism group. *Sūrikaiseikikenkyūsho Kōkyūroku*, (1267):112–141, 2002. Communications in arithmetic fundamental groups (Kyoto, 1999/2001).

- [17] F. Oort. Hyperelliptic supersingular curves. In *Arithmetic algebraic geometry (Texel, 1989)*, volume 89 of *Progr. Math.*, pages 247–284. Birkhäuser Boston, Boston, MA, 1991.
- [18] Tanush Shaska and Helmut Völklein. Elliptic subfields and automorphisms of genus 2 function fields. In *Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000)*, pages 703–723. Springer, Berlin, 2004.
- [19] G. van der Geer and M. van der Vlugt. Fibre products of artin-schrier curves and generalized hamming weights of codes. *Journal of Combinatorial Theory, Series A*, 1995.
- [20] H. Zhu. Hyperelliptic curves of every 2-rank without extra automorphisms. *Proc. Amer. Math. Soc.*, 134, 2006.