4-7-2010

Codes from Riemann-Roch Spaces for Y2 = Xp - X over GF(P)

Darren B. Glass
Gettysburg College

David Joyner
United States Naval Academy

Amy Ksir
United States Naval Academy

Glass, Darren B., David Joyner, and Amy Ksir. "Codes from Riemann-Roch Spaces for Y2 = Xp - X over GF(P)." *International Journal of Information and Coding Theory* 1, no. 3 (2010): 298-312.

Codes from Riemann-Roch Spaces for Y2 = Xp - X over GF(P)

Abstract

Let X denote the hyperelliptic curve y2 = xp - x over a field F of characteristic p. The automorphism group of X is G = PSL(2, p). Let D be a G-invariant divisor on X(F). We compute explicit F-bases for the Riemann-Roch space of D in many cases as well as G-module decompositions. AG codes with good parameters and large automorphism group are constructed as a result. Numerical examples using GAP and SAGE are also given.

Keywords

hyperelliptic curves, AG codes, SL(2, p) representations, Riemann-Roch spaces, automorphisms, automorphism groups, code structure

Disciplines

Mathematics | Non-linear Dynamics | Other Mathematics

CODES FROM RIEMANN-ROCH SPACES FOR $Y^2 = X^P - X$ OVER $GF(P)$

Darren B Glass
Department of Mathematics, Gettysburg College, Gettysburg PA 17325
`dglass@gettysburg.edu`

David Joyner
Dept of Mathematics, United States Naval Academy, Annapolis MD
`wdj@usna.edu`

Amy Ksir
Dept of Mathematics, United States Naval Academy, Annapolis MD
`ksir@usna.edu`

Abstract

Let $\mathcal{X}$ denote the hyperelliptic curve $y^2 = x^p - x$ over a field F of characteristic p. The automorphism group of $\mathcal{X}$ is $G = PSL(2, p)$. Let D be a G-invariant divisor on $\mathcal{X}(F)$. We compute explicit F-bases for the Riemann-Roch space of D in many cases as well as G-module decompositions. AG codes with good parameters and large automorphism group are constructed as a result. Numerical examples using GAP and SAGE are also given.

Darren Glass received his PhD in mathematics from the University of Pennsylvania in 2002. He is currently an Associate Professor at Gettysburg College. His research interests include Galois theory, arithmetic geometry, coding theory, and cryptography.

David Joyner received his PhD in mathematics form the University of Maryland in 1983. He is a Professor at the United States Naval Academy. His interests include coding theory and SAGE development.

Amy Ksir received her PhD in mathematics from the University of Pennsylvania in 1999. She is an Associate Professor at the United States Naval Academy. In 2009 she was a winner of the MAA's Merten M. Hasse Prize and Lester R. Ford Award for her expository paper "Enumerative Algebraic Geometry of Conics," coauthored with Andrew Bashelor and Will Traves.

1 Introduction

The construction of an AG code from a divisor on an algebraic curve is well known. In the case where the curve has a nontrivial automorphism group, and the divisor is invariant under this group, the resulting AG code also has automorphisms. This group of automorphisms can aid in understanding the structure of the code and possibly with more efficient decoding algorithms; see for example [J]. Thus we are interested in understanding explicitly the action of the automorphism group on the code; this is given (via the evaluation map) as the action of the automorphism group on the Riemann-Roch space of the divisor.

To be more precise, let $\mathcal{X}$ be a non-singular projective curve over a field F, and let G be (a finite subgroup of) the automorphism group of $\mathcal{X}$. Let D be a G-invariant divisor on $\mathcal{X}$, and let

$$L(D) = \{f \in F(X) \mid div(f) + D \geq 0\} \cup \{0\}.$$

Then $L(D)$ is a finite-dimensional G-module.

Question: What are these representations? Can we compute their character? Their multiplicities?

In the case where $F = \mathbb{C}$ and D is a canonical divisor, the group action is on the space of holomorphic differentials. In this case, the multiplicity of an irreducible representation is given by the Chevalley-Weil formula (Chevalley and Weil, 1934); the trace of an individual element can be computed using the Eichler trace formula (see for example (Farkas and Kra, 1980)). In the 1980's, (Nakajima, 1984) and (Kani, 1986) gave much more general results. Consider a tamely ramified Galois cover $\pi : \mathcal{X} \to \mathcal{Y} = \mathcal{X}/G$ defined over any algebraically closed field. Then for any divisor D, they were able to compute the character of $L(D)$. (In fact their results generalize beyond curves to higher dimensions, and beyond divisors to any coherent sheaf; but that does not concern us here.)

However, in the case where the field F has positive characteristic p, and p divides the order of G, both the geometry and the representation theory become more complicated. For one thing, the ramification may not be tame. Even in the wild case, the results of Nakajima and Kani can be extended to compute the Brauer character of $L(D)$ (Bourne, 2003). However, the Brauer character does not provide complete information about the representation.

In this paper, we shall focus our attention on one example of this "wild characteristic" situation. This is an interesting family of Artin-Schreier covers which have p-rank 0 and for which the Artin-Schreier automorphism is not in the center of the automorphism group. This family also gives rise to an interesting class of codes, discussed in §3.

2 A wild hyperelliptic curve

Throughout this section, we let $p \geq 3$ be a prime, $F_1 = GF(p)$ be a field of order p, and $\overline{F_1}$ be its algebraic closure. Let $\mathcal{X}$ denote the curve defined by

$$y^2 = x^p - x$$

over an extension F of F_1. $\mathcal{X}$ has genus $\frac{p-1}{2}$. We will also sometimes refer to the weighted projective model (X, Y, Z) ($x = X/Z$, $y = Y/Z^{g+1}$) with weights

1, $g+1=\frac{p+1}{2}$, and 1, in which the point at infinity is nonsingular: $Y^2 = X^pZ - XZ^p$. We compute explicit F-bases for the Riemann-Roch space of certain G-invariant divisors as well as G-module decompositions.

$\mathcal{X}$ has $p+1$ F_1-rational points. Indeed, say $P \in \mathcal{X}(F_1)$ is not the point at infinity, so $P=(x,y)$, for some $x,y \in F_1$. By Fermat's Little Theorem, $x^p - x = 0$, so $y=0$. There are p such points.

We will also be interested in the rational points of $\mathcal{X}$ over a quadratic extension of F_1. Let $a \in \overline{F_1}^\times$ be a primitive $2(p-1)$st root of unity, and let $F_2 = F_1(a) \cong GF(p^2)$.

Lemma 2.1

- *If $p \equiv 1 \pmod 4$ then the rational points of $y^2 = x^p - x$ defined over F_2 are exactly the points which are rational over F_1.*
- *If $p \equiv 3 \pmod 4$ then $\mathcal{X}$ has an additional $2(p^2-p)$ rational points.*

Proof: In $F_2 \cong GF(p^2)$, Euler's criterion tells us that a number α is a quadratic residue if $\alpha^{\frac{p^2-1}{2}} = 1$ and a nonresidue if it is -1. We wish to determine whether, given an $x \in F_2 - F_1$, $x^p - x$ will be a residue. So we notice that $(x^p-x)^p = x^{p^2} - x^p = -(x^p - x)$ and compute:

$$\begin{aligned}(x^p-x)^{\frac{p^2-1}{2}} &= \left[(x^p-x)^{p+1}\right]^{\frac{p-1}{2}}\\ &= \left[(x^p-x)^p(x^p-x))\right]^{\frac{p-1}{2}}\\ &= \left[-(x^p-x)^2\right]^{\frac{p-1}{2}}\\ &= (-1)^{\frac{p-1}{2}}(x^p-x)^{p-1}\\ &= (-1)^{\frac{p+1}{2}}.\end{aligned}$$

Therefore, $x^p - x$ is a quadratic residue if and only if $p \equiv 3 \bmod 4$. In this case, for all choices of $x \in F_2 - F_1$ there will be two values of y on the curve. □

The canonical divisor K has degree $p-3$. Indeed, Hurwitz' formula ((Hartshorne, 1977), page 301) for the degree 2 morphism from $\pi : \mathcal{X} \to \mathbb{P}^1$ says that a canonical divisor K satisfies

$$K = R + \pi^{-1}(K_{\mathbb{P}^1}),$$

where R denotes the ramification divisor and $K_{\mathbb{P}^1}$ denotes a canonical divisor on $\mathbb{P}^1$. The ramification divisor is simply the formal sum of the set of the $p+1$ F_1-rational points discussed above. The canonical divisor on $\mathbb{P}^1$ is given by $K_{\mathbb{P}^1} = -2Q$, for any point Q on $\mathbb{P}^1$. The pull-back of this degree -2 divisor has degree -4, so $\deg(K) = \deg(R) + \deg(\pi^{-1}(K_{\mathbb{P}^1})) = p+1-4 = p-3$.

2.1 Automorphism group and orbits

Over the algebraic closure $\overline{F_1}$ of $F_1 = GF(p)$, we have a short exact sequence,

$$1 \to Z \to \overline{G} \to G \to 1, \tag{1}$$

where $\overline{G} = \mathrm{Aut}_{\overline{F}_1}(\mathcal{X})$, Z is the center of $\overline{G}$ and is generated by the hyperelliptic involution, and $G \cong PGL(2,p)$ (see (Göb, 2003)). The group $PGL(2,p)$ acts on the x-line, or in the weighted projective model on the $[X:0:Z]$ line.

The following transformations are generating elements of $\overline{G}$:

$$\begin{array}{ll} \gamma_1 = \begin{cases} x \longmapsto x, \\ y \longmapsto -y, \end{cases}, & \gamma_2 = \gamma_2(a) = \begin{cases} x \longmapsto a^2 x, \\ y \longmapsto ay, \end{cases} \\ \gamma_3 = \begin{cases} x \longmapsto x+1, \\ y \longmapsto y, \end{cases}, & \gamma_4 = \begin{cases} x \longmapsto -1/x, \\ y \longmapsto y/x^{\frac{p+1}{2}}. \end{cases} \end{array} \tag{2}$$

Except for γ_2, these morphisms are defined over $F_1 = GF(p)$; let $F_2 = F_1(a) \cong GF(p^2)$. Then $\gamma_2(a)$ is defined over F_2. Note that $Z = \langle \gamma_1 \rangle$. The correspondence $G \cong PGL(2,p)$ is:

$$\gamma_2(a) \leftrightarrow \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}_* = \begin{pmatrix} a^2 & 0 \\ 0 & 1 \end{pmatrix}_*,$$

$$\gamma_3 \leftrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}_*,$$

$$\gamma_4 \leftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}_*,$$

where $g \longmapsto g_*$ denotes the quotient $GL(2,p) \to PGL(2,p)$.

Now we describe the automorphism group of $\mathcal{X}$ over $F_1 = GF(p)$. Since $GF(p)$ contains a primitive $(p-1)^{st}$ root of unity, but not a primitive $2(p-1)^{st}$ root of unity, $\mathrm{Aut}_{F_1}(\mathcal{X})$ is a proper subgroup of the entire "absolute Galois group of $\mathcal{X} \to \mathbb{P}^1$". The automorphism group $\mathrm{Aut}_{F_1}(\mathcal{X})$ is a central 2-fold cover of $PSL(2,p)$. In fact, we have $\mathrm{Aut}_{F_1}(\mathcal{X}) \cong SL(2,p)$. This group acts transitively on

$$\mathcal{X}(F_1) = \{(1:0:0), (0:0:1), (1:0:1), ..., (p-1:0:1)\}$$

so it has a single orbit of size $|\mathcal{X}(F)| = p+1$.

Note every point in $\mathcal{X}(F_1)$ is a ramification point of the covering $\mathcal{X} \to \mathcal{X}/\overline{G}$ in the sense that each stabilizer $\overline{G}_P = \mathrm{Stab}_{\overline{G}}(P)$ is non-trivial, $P \in \mathcal{X}(F)$.

Over $F_2 = GF(p^2)$ (or any extension of $F_1 = GF(p)$ containing F_2), the automorphism group is as in (1). The automorphism group $\mathrm{Aut}_{F_2}(\mathcal{X})$ is a central 2-fold cover of $PGL(2,p)$.

Proposition 2.2 *The orbit structure on $\mathcal{X}(F_2)$ is as follows:*

(a) Case $p \equiv 1 \pmod 4$:

The automorphism group of $\mathcal{X}/F_2$ acts transitively on $\mathcal{X}(F_2)$ and the stabilizer of any point is a group of order $2p(p-1)$.

(b) Case $p \equiv 3 \pmod 4$:

Let $P_1 = [1:0:1]$ and fix some $P_2 \in \mathcal{X}(F_2) - \mathcal{X}(F_1)$. The set of rational points $\mathcal{X}(F_2)$ decomposes into a disjoint union of two orbits

$$O_1 = \mathcal{X}(F_1) = G \cdot P_1, \qquad O_2 = \mathcal{X}(F_2) - \mathcal{X}(F_1) = G \cdot P_2,$$

with $|O_1| = p+1$ and $|O_2| = 2p(p-1)$.

Proof: In the first case, where $p \equiv 1 \bmod 4$, the rational points over F_2 are the same as the rational points over F_1 (as stated in Lemma 2.1) so $\mathrm{Aut}_{F_2}(\mathcal{X})$ acts transitively on points of $\mathcal{X}(F_2)$. Since the order of $PGL(2,p)$ is $(p+1)(p^2-p)$, the stabilizer of each point is a group of order $2p(p-1)$.

In the second case, where $p \equiv 3 \pmod 4$, note first that all elements of $\mathrm{Aut}_{F_2}(\mathcal{X})$ preserve $\mathcal{X}(F_1)$, yielding the first orbit. Now using the isomorphism $F_2 = F_1(a)$, we can write two arbitrary elements x_1 and x_2 in $F_2 - F_1$ as $x_i = b_i a + c_i$ (for $i = 1,2$), where b_i and c_i are elements of F_1 and b_i is nonzero. Then γ_2 and γ_3 can be combined to send x_1 to x_2, so the action on $\mathcal{X}(F_2) - \mathcal{X}(F_1)$ is transitive. Again, using the order of $PGL(2,p)$ gives us the order of the stabilizers. □

Remark 2.3 *We learned of these facts from Bob Guralnick.*

Because of the orbit structures described above, we will be looking for bases of the Riemann-Roch spaces of the divisors

$$D_1 = \sum_{P \in \mathcal{X}(F_1)} P,$$

and

$$D_2 = \sum_{P \in \mathcal{X}(F_2) - \mathcal{X}(F_1)} P$$

and their integer linear combinations.

2.2 Representation theory

In characteristic p, the irreducible $SL(2,p)$-modules are known explicitly (Alperin, 1986). They occur in degrees 1, 2, ..., p. If we let

$$V_n = \{\sum_i a_i X^i Z^{n-i}\},$$

where the action of $\overline{G}$ is by $(X,Z) \longmapsto A * (X,Z)^t$, for $A \in \overline{G}$, then the irreducible modules are $V_0, \ldots, V_{p-1}$. The degree of V_n is $n+1$. Note that $\mathrm{tr}\, V_m(t) = \mathrm{tr} V_n(t)$ if and only if $m+n = p-1$, where $t = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$.

The irreducible $PGL(2,p)$ modules can be determined from these as follows. First we pass to $PSL(2,p) \equiv SL(2,p)/\pm 1$, and observe that the irreducible representations of $PSL(2,p)$ are simply the irreducible representations of $SL(2,p)$ on which $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ acts trivially. These are the V_n with n even.

Now we extend to $PGL(2,p)$. We can divide the conjugacy classes of $PGL(2,p)$ into two types. Let M be a matrix in $GL(2,p)$, and M_* its class in $PGL(2,p)$. If $\det(M)$ is a quadratic residue $\pmod p$, then the determinant of any other matrix in M_* will also be a quadratic residue mod p. In particular, $\frac{1}{\sqrt{\det M}}M$ is in $SL(2,p)$, and represents the same class M_* in $PGL(2,p)$. If $\det(M)$ is not a quadratic residue mod p, we can multiply by $\gamma_2(a) = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, where a is not a square mod p, to get a matrix equivalent to an element of $SL(2,p)$. So the action of an element of $PGL(2,p)$ will be determined by the action of $PSL(2,p)$ and $\gamma_2(a)$. Let ψ be the degree 1 module where the matrices with determinant a quadratic-residue act trivially and $\gamma_2(a)$ acts as multiplication by -1. Then the irreducible representations of $PGL(2,p)$ are $V_0, V_2, \ldots, V_{p-1}$ (even degrees only), and $V_0 \otimes \psi, V_2 \otimes \psi, \ldots, V_{p-1} \otimes \psi$ (even degrees only).

2.3 Function field background and main question

Background on the function field $K = F_1(\mathcal{X}) = F_1(x,y)$ of this curve from (Stichtenoth, 1993), §VI.4:

(a) $[K : F_1(y)] = p$, so as an F_1-vector space

$$F_1(x,y) = F_1(y) \oplus xF_1(y) \oplus \ldots \oplus x^{p-1}F_1(y).$$

(b) $K/F_1(y)$ is Galois and

$$\begin{array}{ccc} Gal(K/F_1(y)) & = & F_1 \\ \sigma & \mapsto & a \\ \sigma(x) = x + a & & \end{array}$$

(c) The pole P_∞ of y in $F_1(y)$, a place on the projective line $\mathbb{P}^1$, has a unique extension Q_∞, a place of $\mathcal{X}$, which is totally ramified, $e(Q_\infty/P_\infty) = p$. Q_∞ is a place of $\mathcal{X}$ of degree 1, corresponding to the point [1, 0, 0] in the projective model.

(d) P_∞ is the only place of $\mathbb{P}^1$ which ramifies with respect to the projection map $\mathcal{X} \to \mathbb{P}^1$, $(x,y) \longmapsto y$.

(e) $(dy)_\infty = (p-3)Q_\infty$,

(f) $(x)_\infty = 2Q_\infty$, $(y)_\infty = pQ_\infty$.

(g) $L(rQ_\infty) = Span[\ x^i y^j \mid 2i + pj \leq r, 0 \leq i, 0 \leq j \leq p-1\ ]$.

Let

$$D_1 = \sum_{P \in \mathcal{X}(F_1)} P,$$

so $\deg(D_1) = |\mathcal{X}(F_1)| = p + 1 = 2g + 2$ and therefore rD_1 is non-special for each $r \geq 1$. In particular,

$$\dim L(rD_1) = \deg(rD_1) - g + 1 = r(p+1) - \frac{p-3}{2} = (2r-1)g + 2r + 1.$$

Taking $r = 1$ for instance, we have $\dim L(D_1) = \frac{p+5}{2} = g + 3$. Each successive quotient $L((r+1)D_1)/L(rD_1)$ has dimension $p + 1 = 2g + 2$, $r \geq 1$. The vector space $L(rD_1)$ is a $\overline{G}$-module, hence so is each such quotient. Indeed, the hyperelliptic involution acts trivially on $\mathcal{X}(F_1)$, so this action actually factors through an action of G.

Question: Is $L(D_1)$ an irreducible G-module or $\overline{G}$-module? Is the quotient $L((r+1)D_1)/L(rD_1)$ an irreducible G-module or $\overline{G}$-module?

Answer: We shall see explicitly that the answer is no.

2.4 Module structure over $GF(p)$

Over $GF(p)$ there are $p+1$ rational points: the points of the form $(a, 0)$ for all a along with the point at ∞. Note that G is transitive on this set of points, and therefore the only G-invariant divisors are the divisors of the form rD_1, where D_1 is the sum of all $p+1$ points defined over $GF(p)$.

The functions we will use to construct bases of the Riemann-Roch spaces $L(rD_1)$ are

$$f_{k,j} = \frac{x^j}{(x^p - x)^k}, \qquad g_{k,j} = \frac{yx^j}{(x^p - x)^k}.$$

Note that $f_{k,j}$ has a pole of order $2k$ at each point $(a, 0)$, $1 \leq a \leq p-1$; a pole of order $2(k-j)$ at $(0,0)$; and a pole of order $2(j-k)$ at Q_∞. Similarly, $g_{k,j}$ has a pole of order $2k-1$ at each point $(a,0)$, $1 \leq a \leq p-1$; a pole of order $2(k-j)-1$ at $(0,0)$; and a pole of order $2(j-k)+p$ at Q_∞.

Consider the vector space

$$B_1 = \mathrm{Span}\{ \frac{yx^j}{x^p - x} \mid 0 \leq j \leq \frac{p+1}{2}\}.$$

There are $\frac{p+3}{2}$ elements in this spanning set, all of which are linearly independent, so that $\dim B_1 = \frac{p+3}{2}$. It is clear that B_1 remains invariant under the action of γ_1, $\gamma_2(a)$, and γ_3. Note that

$$\gamma_4 : \frac{yx^j}{x^p - x} \longmapsto (-1)^{j+1} \frac{yx^{\frac{p+1}{2} - j}}{x^p - x},$$

so B_1 is indeed a $\overline{G}$-module.

Lemma 2.4 *$L(D_1) = B_1 \oplus \mathbf{1}$, as $\overline{G}$-modules. Here the trivial representation $\mathbf{1}$ represents the constant functions.*

Proof: By the above, B_1 is a $\overline{G}$-module. By definition of the Riemann-Roch space, $B_1 \subset L(D_1)$, and $L(D_1)$ contains the constant functions on $\mathcal{X}$. Since D_1 is non-special, the Riemann-Roch theorem tells us that $\dim L(D_1) = 1 + \dim B_1$, and the claimed result follows. □

In order to compute $L(rD_1)$ for $r > 1$ let us make the following definitions:

Definition 2.5 *(a)* $A_k = \mathrm{Span}\{\ f_{k,j}\ \mid 0 \le j \le k(p+1)\}$

(b) $B_k = \mathrm{Span}\{\ g_{k,j}\ \mid 0 \le j \le k(p+1) - \frac{p+1}{2}\}$

Note that this definition agrees with the above definition of B_1 and furthermore $A_0 = \mathbf{1}$. By convention, set $B_0 = \{0\}$.

Lemma 2.6 *$L(rD_1) = A_{\lfloor \frac{r}{2} \rfloor} \oplus B_{\lceil \frac{r}{2} \rceil}$, for $r \ge 1$.*

Proof: It is not hard to verify that both $A_{\lfloor \frac{r}{2} \rfloor}$ and $B_{\lceil \frac{r}{2} \rceil}$ are contained in $L(rD_1)$. Furthermore, one can use (2) to show that A_k and B_k are each G-invariant. Since rD_1 is non-special, the Riemann-Roch theorem allows us to compute $\dim L(rD_1)$, for each $r \ge 1$ and see that increasing r by one increases the dimension by $p+1$. Therefore, the dimensions are correct and the lemma follows. □

It follows immediately from the claim that in order to understand the natural quotient spaces $L(rD_1)/L((r-1)D_1)$ it will suffice to understand the structure of either A_k/A_{k-1} or B_k/B_{k-1}, depending on the parity of r.

Regarding A_k/A_{k-1}, we have the relation

$$f_{k-1,j} = f_{k,j+p} - f_{k,j+1},$$

and there is a similar relation for the $g_{k,j}$'s. Using these relations, we can show the following:

Lemma 2.7 *There is a basis of A_k/A_{k-1} represented by the functions*

$$\{f_{k,j} \mid 0 \le j \le p-1\} \cup \{f_{k,k(p+1)}\}.$$

Similarly, there is a basis of B_k/B_{k-1} represented by the functions

$$\{g_{k,j} \mid 0 \le j \le p-1\} \cup \{g_{k,k(p+1)}\}.$$

Lemma 2.8 *The G-module A_1 has three irreducible composition factors. First the constants form a one-dimensional factor. There is a three-dimensional factor with basis $\frac{1}{x^p - x}$, $\frac{x + x^p}{x^p - x}$, and $\frac{x^{p+1}}{x^p - x}$, which is isomorphic to V_2. Then there is a $p-2$-dimensional factor. This one must be isomorphic to V_{p-3}.*

Proof: The hyperelliptic involution acts trivially on A_1, so we can consider the action of $PSL(2,p)$. The constants are clearly invariant. The three-dimensional space is invariant too, and since it's three-dimensional and irreducible it must be isomorphic to V_2. The proof that the remaining quotient G-module, call it A_1^*, is irreducible is a rather elaborate computation explicitly showing $A_i^* \cong V_{p-3}$. The several pages of tedious computation is omitted. (A much easier character computation suggests this but since characters do not determine equivalence classes of G-modules in characteristic p, this is not sufficient.) $\square$

2.5 Module structure over $GF(p^2)$

Any G-invariant divisor on $\mathcal{X}(F_2)$ should look like $D = rD_1 + sD_2$ where D_i is the sum of all points in O_i. The previous section made sense of $L(rD_1)$, so it makes sense to first consider the structure of $L(sD_2)$.

Let us define the following as above:

Definition 2.9 *If* $p \equiv 3 \pmod 4$, *let*

(a) $A'_k = \mathrm{Span}\{ \frac{x^j(x^p-x)^k}{(x^{p^2}-x)^k} \mid 0 \le j \le k(p^2-p)\}$

(b) $B'_k = \mathrm{Span}\{ \frac{yx^j(x^p-x)^k}{(x^{p^2}-x)^k} \mid 0 \le j \le k(p^2-p) - \frac{p+1}{2}\}$

One can check that these are still G-invariant and that they have the right poles. Next, we state the analog of the first Claim.

Lemma 2.10 *(a) If* $p \equiv 1 \pmod 4$, $L(rD_1) = A_{\lfloor \frac{r}{2} \rfloor} \oplus B_{\lceil \frac{r}{2} \rceil}$, *for* $r \ge 1$.

(b) If $p \equiv 3 \pmod 4$, $L(rD_1 + sD_2) = A_{\lfloor \frac{r}{2} \rfloor} \oplus B_{\lceil \frac{r}{2} \rceil} \oplus A'_s \oplus B'_s$, *for* $r, s \ge 1$.

Since both the inclusions and the dimension count are essentially trivial, the proof of this lemma is left to the reader.

The situation for A'_k/A'_{k-1} and B'_k/B'_{k-1} is a bit more complicated than in Lemma 2.7 (see previous section). In this case,

$$A'_k = \langle f'_{k,j} \mid 0 \le j \le k(p^2-p) \rangle,$$

and

$$B'_k = \langle g'_{k,j} \mid 0 \le j \le k(p^2-p) - \frac{p+1}{2} \rangle,$$

where

$$f'_{k,j} = \frac{x^j(x^p-x)^k}{(x^{p^2}-x)^k}, \qquad g'_{k,j} = \frac{yx^j(x^p-x)^k}{(x^{p^2}-x)^k}.$$

Regarding A'_k/A'_{k-1}, we have the relation

$$f'_{k-1,j} = \sum_{m=0}^{p} f_{k,j+m(p-1)}.$$

Using these, it can be shown that there is a basis of A'_k/A'_{k-1} represented by the functions

$$\{f'_{k,j} \mid 0 \leq j \leq p^2 - p\}.$$

3 A family of codes

Consider a prime $p > 3$ with $p \equiv 3 \pmod 4$. Let $\mathcal{X}$, O_1 and O_2 be as in Proposition 2.2 above, and D_1 and D_2 be as in Section 2.5. Fix some labeling $O_2 = \{P_1, ..., P_n\}$ (so $D_2 = \sum_{i=1}^{n} P_i$) and let $r \geq 1$ be an integer. Let $C = C(rD_1, D_2)$ denote the AG code which is the image of $L(rD_1)$ under the evaluation map $f \longmapsto (f(P_1), \ldots, f(P_n))$. Note that $\deg D_1 = (p+1)$ and $\deg D_2 = 2p^2 - 2p$, so if $r < (2p^2 - 2p)/(p+1)$, then the evaluation map is injective.

Proposition 3.1 *Let r be an integer with $1 \leq r < (2p^2 - 2p)/(p+1)$, then the code $C = C(rD_1, D_2)$ has parameters $[n, k, d]$ as follows:*

$$n = |O_2| = 2p^2 - 2p, \qquad k = r(p+1) - (p-1)/2 + 1, \qquad d = 2p^2 - 2p - r(p+1).$$

Proof: The value for n is by definition. The Riemann-Roch theorem gives the dimension of $L(rD_1)$; since $r \geq 1$, $\deg rD_1 \geq p+1 > 2g-2$ so rD_1 is nonspecial and $\dim L(rD_1) = r(p+1)+1-(p-1)/2$. Since the evaluation map is injective, this gives our value for k. By Theorem 3.1.10 in (Tsfasman and Vladut, 1991), we have $d \geq 2p^2 - 2p - r(p+1)$. Using the results of section 2.5, we can find a function in $L(rD_1)$ whose image under the evaluation map is a code word of weight $2p^2 - 2p - r(p+1)$, making this into an equality, as follows.

If f is a function of $L(rD_1)$, then it is the sum of a function in $A_{\lfloor \frac{r}{2} \rfloor}$ and a function in $B_{\lceil \frac{r}{2} \rceil}$; in other words

$$f = \frac{p(x)}{(x^p - x)^{\lfloor \frac{r}{2} \rfloor (p+1)}} + \frac{q(x)y}{(x^p - x)^{\lceil \frac{r}{2} \rceil (p+1)}}. \tag{1}$$

where $p(x)$ and $q(x)$ are polynomials. If r is odd, then the degree of $q(x)$ is larger than the degree of $p(x)$, and if r is even then the opposite is true; in either case the degree of the larger of the two polynomials is $r\frac{p+1}{2}$. To make a code word of minimal weight, we take the smaller degree polynomial to be 0, and make the other a product of $r\frac{p+1}{4}$ distinct quadratic factors which are irreducible over $F_1 = GF(p)$. (The upper bound on r guarantees the existence of the factors). The zeroes of f will then include four points of O_2 for each factor, for a total of $r(p+1)$ points. On the other points of O_2, f will not vanish, so the weight of the resulting code word will be $\deg D_2 - r(p+1) = 2p^2 - 2p - r(p+1)$, as desired. $\square$

These codes are G-invariant since both D_1 and D_2 are. In fact, the G-module decomposition for $L(rD_1)$ established in §2.5 applies to C as well, since the evaluation map $L(rD_1) \to C$ is G-equivariant.

We also obtain the following asymptotic result.

Corollary 3.1 *If $r = p$ then the automorphism group G of C has order $> n^{3/2}/2$ and the asymptotic parameters $\delta = d/n$ and $R = k/n$ satisfy*

$$\delta = \frac{1}{2} + O(1/p), \qquad R = \frac{1}{2} + O(1/p),$$

as $p \to \infty$.

This family of codes was discussed in the conjectural paper (Joyner, 2005), though without proof, and a possible decoding algorithm for these codes can be found there.

4 Computational examples

This section is included to emphasize the effective computational manner of the results above. We use `GAP` and `SAGE` in our computations below.

The `SAGE` files for the examples below, and others, can be found at `http://sage.math.washington.edu/home/wdj/research/sage/`.

The previous section constructed codes arising from Proposition 2.10. If one uses instead a one-point code, then there is no assurance that the automorphism group will be nearly as large, as the example below illustrates. For more on the relationship between automorphism groups of curves and codes, see (Joyner and Ksir, 2007).

Example 4.1 *Let $F = GF(7)$ and let $\mathcal{X}$ denote the curve defined by*

$$y^2 = x^7 - x.$$

This has genus 3. The automorphism group G is a central 2-fold cover of $PSL_2(F)$: we have a short exact sequence,

$$1 \to Z \to G \to PSL_2(7) \to 1,$$

where Z denotes the subgroup of G generated by the hyperelliptic involution (which happens to also be the center of G). (Over the algebraic closure $\overline{F}$, $\mathrm{Aut}_{\overline{F}}(\mathcal{X})$/center $\cong PGL_2(\overline{F})$, by (Göb, 2003), Theorem 1.) The following transformations are elements of $\mathrm{Aut}_F(\mathcal{X})$:

$$\gamma_1 = \begin{cases} x \longmapsto x, \\ y \longmapsto -y, \end{cases}, \quad \gamma_2 = \begin{cases} x \longmapsto a^2 x, \\ y \longmapsto ay, \end{cases} \quad (\ a \in F^\times),$$
$$\gamma_3 = \begin{cases} x \longmapsto x+1, \\ y \longmapsto y, \end{cases}, \qquad \gamma_4 = \begin{cases} x \longmapsto -1/x, \\ y \longmapsto y/x^4, \end{cases},$$

where we may take $a = 2$. There are 8 F-rational points:

$$\mathcal{X}(F) = \{P_1 = (1:0:0), P_2 = (0:0:1), P_3 = (1:0:1), ..., P_8 = (6:0:1)\}.$$

The automorphism group acts transitively on $\mathcal{X}(F)$*. Consider the projection* $\mathcal{X} \to \mathbb{P}^1$ *defined by* $\phi(x, y) = x$*. The map* ϕ *is ramified at every point in* $\mathcal{X}(F)$ *and at no others.*

All the stabilizers $H_i = Stab(P_i, G)$ *are conjugate to each other in* G*,* $1 \leq i \leq 8$*. Let* $B = H_1 = Stab(P_1, G)$ *denote the stabilizer of the point at infinity in* $\mathcal{X}(F)$*. The group* G *is a non-abelian group of order* 42 *(In fact, the group* $B/Z(B)$ *is the non-abelian group of order* 21*, where* $Z(H)$ *denotes the center of* H*.)*

It is known (Proposition VI.4.1, (Stichtenoth, 1993)) that, for each $m \geq 1$*, the Riemann-Roch space* $L(mP_1)$ *has a basis consisting of monomials,*

$$x^i y^j, \qquad 0 \leq i \leq 6,\ j \geq 0,\ 2i + 7j \leq m.$$

Let $D = 5P_1$*,* $E = \mathcal{X}(F) - \{P_1\}$*, and let*

$$C = C(D, E) = \{(f(P_2), ..., f(P_8)) \mid f \in L(D)\}.$$

This is a $(7, 3, 5)$ *code over* F*. In fact,* $\dim(L(D)) = 3$*, so the evaluation map* $f \longmapsto (f(P_2), ..., f(P_8))$*,* $f \in L(D)$*, is injective. Since* B *fixes* D *and preserves* S*, it acts on* C *via*

$$g : (f(P_2), ..., f(P_8)) \longmapsto (f(g^{-1}P_2), ..., f(g^{-1}P_8)),$$

for $g \in B$*.*

Let P *denote the permutation group of this code. It a group of order* 42*. However, it is not isomorphic to* B*. In fact,* P *has trivial center. The (permutation) action of* G *on this code implies that there is a homomorphism*

$$\psi : H_1 \to P.$$

What is the kernel of this map?

GAP will narrow the choices down to two possibilities: either a subgroup of order 6 *or a subgroup of order* 21 *(this is obtained by matching possible orders of quotients* H_1/N *with possible orders of subgroups of* P*). Take the automorphisms* γ_1*,* $\gamma_2 = \gamma_2(2)$ *(*$a = 2$*) and* γ_3*. If we identify* $S = \{P_2, ..., P_8\}$ *with* $\{1, 2, ..., 7\}$ *then*

$$\gamma_1 \leftrightarrow (2, 7)(3, 6)(4, 5) = g_1,$$

$$\gamma_2 \leftrightarrow (2, 5, 3)(4, 6, 7) = g_2,$$

$$\gamma_3 \leftrightarrow (1, 2, ...7) = g_3.$$

The group $N = \langle g_2, g_3 \rangle$ *is a non-abelian normal subgroup of* $H_1 = \langle g_1, g_2, g_3 \rangle$ *of order* 21*.*

The character table (over $\mathbb{C}$*) of* N *is*

Class	1	2	3	4	5
Size	1	7	7	3	3
Order	1	3	3	7	7
$p = 7$	1	2	3	1	1
χ_1	1	1	1	1	1
χ_2	1	ω	$-1-\omega$	1	1
χ_3	1	$-1-\omega$	ω	1	1
χ_4	3	0	0	ζ	ζ^3
χ_5	3	0	0	ζ^3	ζ

where ω denotes a cube root of unity and $\zeta \neq 0$ is a root of unity which will be unimportant for our example. According to `GAP`*, the character table (over F) of N is*

χ_{1a}	1	1	1	1	1
χ_{1b}	1	ω^2	ω	1	1
χ_{1c}	1	ω	ω^2	1	1

where the ordering on the conjugacy classes is the same. Note that the last two conjuacy classes are irregular mod 7.

Finally, we compute the matrix representation of B on $L(D)$, where $D = 5P_1$. First, note that γ_1 acts as the identity,

$$\gamma_2 : \begin{pmatrix} 1 \\ x \\ x^2 \end{pmatrix} \longmapsto \begin{pmatrix} 1 \\ 4x \\ 2x^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ x \\ x^2 \end{pmatrix},$$

and

$$\gamma_3 : \begin{pmatrix} 1 \\ x \\ x^2 \end{pmatrix} \longmapsto \begin{pmatrix} 1 \\ x+1 \\ (x+1)^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ x \\ x^2 \end{pmatrix}.$$

In fact, every element of N may be written $g_2^i g_3^j$, $0 \leq i \leq 2$, $0 \leq j \leq 6$. The conjugacy classes of N are represented by $1, g_2, g_2^2, g_3, g_3^3$. The matrices of the representation ρ of B acting on $L(D)$ are

$$\rho(1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho(g_2) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad \rho(g_2^2) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix},$$
$$\rho(g_3) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix}, \quad \rho(g_3^3) = \begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 2 & 6 & 1 \end{pmatrix}.$$

This is not a semisimple representation, but it is solvable. In particular, B is solvable.

The character table of N implies that the the semisimplification ρ_{ss} is the direct sum of the three one-dimensional representations: $\mathrm{tr}\rho_{ss} = \chi_{1a} + \chi_{1b} + \chi_{1c}$.

Example 4.2 *Next, we give an example involving the codes constructed from Proposition 2.2(a). In this example, we show how* SAGE *can be used to compute an* $[84, 5, 77]$*-code over* $GF(49)$ *using the Riemann-Roch spaces computed above.*

SAGE

```
sage: p = 7
sage: F = GF(p)
sage: E.<a> = GF(p^2,"a")
sage: M = MatrixSpace(E,2,2)
sage: M1 = MatrixSpace(F,2,2)
sage: V = VectorSpace(E,2)
sage: X = ProjectiveSpace(1,E)
```

This lays down the basics - the group acting and base fields.

Now we define the curve and compute points on it (which is implicitly using Singular).

SAGE

```
sage: R.<x> = PolynomialRing(E,"x")
sage: f = x^p-x
sage: C = HyperellipticCurve(f)
sage: pts = C.rational_points()
sage: ptsF = [pt for pt in pts if not("a" in str(pt[0])\
 or "a" in str(pt[1]) or "a" in str(pt[2]))]
sage: ptsE = [pt for pt in pts if not(pt in ptsF)]
sage: len(pts); len(ptsF); len(ptsE)
92
8
84
```

These sets are group orbits and have the size predicted by Proposition 2.2 above. We take $r = 1$ *and compute* $L(rD_1)$ *using Lemma 2.6 below. The set* `ptsE` *represents* O_2*.*

SAGE

```
sage: R2.<x,y> = PolynomialRing(E,"x,y")
sage: FracR2 = FractionField(R2)
sage: bA0 = FracR2(1)
sage: bB1_0 = FracR2(y/(x^p-x))
sage: bB1_1 = FracR2(y*x/(x^p-x))
sage: bB1_2 = FracR2(y*x^2/(x^p-x))
sage: bB1_3 = FracR2(y*x^3/(x^p-x))
sage: bB1_4 = FracR2(y*x^4/(x^p-x))           # basis for A_0
\oplus B_1
sage: r1 = [bA0(pt[0],pt[1]) for pt in ptsE]
sage: r2 = [bB1_0(pt[0],pt[1]) for pt in ptsE]
sage: r3 = [bB1_1(pt[0],pt[1]) for pt in ptsE]
sage: r4 = [bB1_2(pt[0],pt[1]) for pt in ptsE]
sage: r5 = [bB1_3(pt[0],pt[1]) for pt in ptsE]
sage: r6 = [bB1_4(pt[0],pt[1]) for pt in ptsE]
sage: MS = MatrixSpace(E,6,len(ptsE))
sage: Ggenmat = MS([r1,r1,r3,r4,r5,r6])
sage: Cagcode = LinearCode(Ggenmat)
```

```
sage: Cagcode
Linear code of length 84, dimension 5 over Finite Field in a of size
7^2
sage: time Cagcode.minimum_distance()
CPU times: user 0.32 s, sys: 0.01 s, total: 0.33 s
Wall time: 238.86 s
77
```

5 A bigger wild family of curves: Open questions

The hyperelliptic curve studied in the previous section is an example of a family of curves defined over $GF(p)$ of the form

$$y^m = x^p - x,$$

where m is any proper divisor of $p+1$. This curve will have genus $\frac{(p-1)(m-1)}{2}$ and will have p-rank equal to zero (in fact it will actually be superspecial). These curves, which over $GF(q^2)$ can be viewed as quotients of the Hermitian curve $y^q = x^q + x$, have been studied by a number of authors, including (Henn, 1978) and (Valentini and Madan, 1980), who showed that these curves were one of a small number of curves in which the Artin-Schreier automorphism is not in the center of the automorphism group. They further show that the automorphism group of this curve is an extension of $\mathbb{Z}/m\mathbb{Z}$ by $PGL(2,p)$. One can easily check that a curve of this form will have the following automorphisms defined over $GF(p^m)$:

$$\begin{aligned} \gamma_1 &= \begin{cases} x \longmapsto x, \\ y \longmapsto \zeta y, \end{cases}, & \gamma_2 = \gamma_2(a) &= \begin{cases} x \longmapsto a^m x, \\ y \longmapsto ay, \end{cases} \\ \gamma_3 &= \begin{cases} x \longmapsto x+1, \\ y \longmapsto y, \end{cases}, & \gamma_4 &= \begin{cases} x \longmapsto -1/x, \\ y \longmapsto y/x^{\frac{p+1}{m}}, \end{cases} \end{aligned} \tag{1}$$

where $\zeta \in F^\times$ is a primitive m^{th} root and $a \in F^\times$ is a primitive $m(p-1)^{st}$ root.

Just as in the hyperelliptic case, the only G-invariant $GF(p)$-rational divisors are the divisors of the form rD_1, where D_1 is the sum of all $p+1$ points defined over $GF(p)$. We define the following vector spaces:

Definition 5.1 *For each k between 0 and $m-1$, let* $A_i^k = \mathrm{Span}\{ \frac{x^j y^k}{(x^p - x)^i} \mid 0 \leq j \leq i(p+1) - \frac{k}{m}(p+1)\}$.

Conjecture 5.2 $L(rD_1) = \bigoplus_{k=0}^{m-1} A^k_{\lfloor \frac{r+k}{m} \rfloor}$.

One can check directly that these functions are in the Riemann-Roch spaces as desired, and therefore it will suffice to show that $L(rD_1)$ and $\bigoplus_{k=0}^{m-1} A^k_{\lfloor \frac{r+k}{m} \rfloor}$ have the same dimensions. It is expected that a proof will be similar to that of Lemma 2.6. We note that if $r \geq m-1$ then $\deg(rD_1) \geq (m-1)(p+1) > (m-1)(p+1) - 2m = 2g-2$. Therefore, rD_1 will be a non-special divisor and one computes that the dimension of $L(rD_1)$ will be $r(p+1) - \frac{(p-1)(m-1)}{2} + 1$. In particular, this verifies the conjecture in this case. We also note that some cases of this conjecture are handled by results in (Matthews, 2005).

In addition to this conjecture, we end the paper with several questions about these curves.

Question 5.1 *What are the reduced G-invariant divisors in the case of G-invariant divisors over $GF(p^m)$, where $m > 2$? What is the analog of Proposition 2.2?*

Question 5.2 *What is the analog of Conjecture 5.2 in the case of G-invariant divisors over $GF(p^m)$, for $m > 2$?*

Question 5.3 *What is the analog of Proposition 3.1? In particular, can one construct G-invariant codes using orbits of points on curves of the form $y^m = x^p - x$ which have good values for their parameters?*

Certain cases of this final question are addressed in (Matthews, 2005).

References

J. Alperin (1986) *Local representation theory*. Cambridge: Cambridge University Press.

N. Borne (2003) *Une formule de Riemann-Roch equivariante pour des courbes,* Can. J. Math. **55**, pp. 693-710.

R. Brauer and C. Nesbitt (1941), *On the modular characters of groups*, Ann. of Math. **42**, pp. 556-590.

C. Chevalley, A. Weil (1934), *Über das Verhalten der Integrale erster Gattung bei Automorphismen des Funktionenkörpers,* Abh. Math. Sem. Univ. Hamburg **10**, pp. 358-361.

H. Farkas and I. Kra (1980), *Riemann Surfaces*, Springer-Verlag, New York.

The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*; `http://www.gap-system.org`.

N. Göb (2003), *Computing the automorphism groups of hyperelliptic function fields,* available at `http://front.math.ucdavis.edu/math.NT/0305284`.

R. Hartshorne (1977), *Algebraic geometry*, Springer-Verlag.

H. W. Henn (1978), *Funktionenkörper mit grober Automorphismengruppe* Jour. Reine Angew. Math. **302**, pp. 96-115.

D. Joyner (2005), *Conjectural permutation decoding of some AG codes,* Communications in Computer Algebra, **39**, pp. 166-172.

D. Joyner and A. Ksir (2005), *Modular representations on some Riemann-Roch spaces of modular curves X(N)*, in *Computational Aspects of Algebraic Curves*, (Editor: T. Shaska) Lecture Notes in Computing, World Scientific Publishing Co. Ltd., Hackensack, NJ.

——— (2007), *Decomposing representations of finite groups on Riemann-Roch spaces,* Proc. Amer. Math. Soc. **135**, pp. 3465-3476.

——— and W. Traves (2007), *Automorphism groups of GRS codes,* in **Advances in coding theory and cryptology, World Scientific** (T. Shaska, W. C. Huffman, D. Joyner, V. Ustimenko, editors) Series on Coding Theory and Cryptology, 2. World Scientific Publishing Co. Ltd., Hackensack, NJ.

E. Kani (1986), *The Galois-module structure of the space of holomorphic differentials of a curve,* J. Reine Angew. Math. **367**, pp. 187-206.

F. J. MacWilliams and N. J. A. Sloane (1977) *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam.

G. L. Matthews (2005), Weierstrass semigroups and codes from a quotient of the Hermitian curve, Designs, Codes, and Crytography vol. 37, no. 3, 473-492.

S. Nakajima (1984), *Galois module structure of cohomology groups of an algebraic variety*, Inv. Math. **75**, pp. 1-8.

SAGE Mathematical Software, Version 4.1,
`http://www.sagemath.org`.

H. Stichtenoth (1993), *Algebraic function fields and codes*, Springer-Verlag.

M. A. Tsfasman and S. G. Vladut (1991), **Algebraic-geometric codes**, Mathematics and its Applications, Kluwer Academic Publishers, Dordrechet.

R. Valentini and M. Madan (1980), *A Hauptsatz of L.E. Dickson and Artin-Schreier extensions*, J. Reine Angew. Math. **318**, pp. 156-177.