

:Automorphism groups of some AG codes

Automorphism groups of some AG codes

David Joyner and Amy Ksir

Abstract

We show that in many cases, the automorphism group of a curve and the permutation automorphism group of a corresponding AG code are the same. This generalizes a result of Wesemeyer beyond the case of planar curves.

Index terms: Algebraic-geometric codes, algebraic curves, code automorphisms, Riemann-Roch spaces.

Automorphism groups of some AG codes

I. INTRODUCTION

THE construction of AG (algebraic-geometric) codes uses the Riemann-Roch space $L(D)$ associated to a divisor D of a curve X defined over a finite field [3]. Typically X has no non-trivial automorphisms, but when it does we may ask how this can be used to better understand AG codes constructed from X .

Conversely, we may ask how the permutation automorphism group of an AG code corresponds with the automorphism group of the curve used to construct the code. In this correspondence we show that, in many cases, the automorphism group of a curve and the permutation automorphism group of a corresponding AG code are in fact the same.

Knowledge of which codes have large automorphism group can have applications to encoding (see [6]) and to decoding (indeed, permutation decoding is implemented in version 2.0 or better of the error-correcting computer algebra package [5]).

In Section II, we introduce notation and review basic properties of AG codes. In Section III, following [12], we introduce some notation and recall some basic properties of group automorphisms on curves and codes (we also take the opportunity to correct a typo in [12] which was copied into [14]). In Section IV, we prove our main results on pulling back code permutations to curve automorphisms. In Section V we use the main theorem and corollary to compute the automorphism groups of codes in several examples.

II. THE RIEMANN-ROCH SPACE $L(D)$ AND THE ASSOCIATED AG CODE

Let X be a smooth projective curve (scheme of dimension 1) over a finite field F , and let $F(X)$ denote the field of rational functions on X . If D is any divisor on X , the Riemann-Roch space $L(D)$ is a finite dimensional F -vector space given by

$$L(D) = L_X(D) = \{f \in F(X)^\times \mid \text{div}(f) + D \geq 0\} \cup \{0\},$$

where $\text{div}(f)$ denotes the (principal) divisor of the function $f \in F(X)$. If \bar{D} denotes the corresponding divisor over the algebraic closure \bar{F} , then $L(\bar{D}) = L(D) \otimes \bar{F}$ [12], [13].

Let $P_1, \dots, P_n \in X(F)$ be distinct points, and let $E = P_1 + \dots + P_n$ be the associated divisor. Let D be a divisor of positive degree on X such that D and E have disjoint support. Let $C = C(D, E)$ denote the AG code

$$C = \{(f(P_1), \dots, f(P_n)) \mid f \in L(D)\}. \quad (1)$$

This is the image of $L(D)$ under the evaluation map

$$\begin{aligned} \text{eval}_E : L(D) &\rightarrow F^n, \\ f &\mapsto (f(P_1), \dots, f(P_n)). \end{aligned} \quad (2)$$

The kernel of the map eval_E is contained in $L(D - E)$, which is 0 if $\text{deg}(E) > \text{deg}(D)$. Thus for $n > \text{deg}(D)$, eval_E defines an isomorphism between $L(D)$ and the code $C(D, E)$.

III. FROM CURVE AUTOMORPHISMS TO CODE AUTOMORPHISMS

Now let G be a group of automorphisms of the curve X , and assume that D and E are both stabilized by G . We will say that $G \subseteq \text{Aut}_{D,E}(X)$. Then G also acts on the code C , as follows.

The action of $\text{Aut}(X)$ on $F(X)$ is defined as:

$$\begin{aligned} \text{Aut}(X) &\longrightarrow \text{Aut}(F(X)), \\ T &\longmapsto (f \longmapsto T^*f) \end{aligned}$$

where for any $P \in X$, $T^*f(P) = f(T^{-1}(P))$. We use T^{-1} rather than T here, to conform to the convention that the action should be on the left: for any $T_1, T_2 \in \text{Aut}(X)$, we want $(T_1 \circ T_2)^*f(P) = T_1^*T_2^*f(P) = T_2^*f(T_1^{-1}(P)) = f(T_2^{-1}(T_1^{-1}(P))) = f((T_1 \circ T_2)^{-1}(P))$.

Of course, $\text{Aut}(X)$ also acts on the group $\text{Div}(X)$ of divisors of X , denoted $T(\sum_P d_P P) = \sum_P d_P T(P)$, for $T \in \text{Aut}(X)$, P a prime divisor, and $d_P \in \mathbb{Z}$. It is easy to see that $\text{div}(T^*f) = T^{-1}(\text{div}(f))$. Because of this, if $\text{div}(f) + D \geq 0$ then $\text{div}(T^*f) + T^{-1}(D) \geq 0$, for all $T \in \text{Aut}(X)$. In particular, if the action of $G \subset \text{Aut}(X)$ on X leaves $D \in \text{Div}(X)$ stable then G also acts on $L(D)$. Assuming that $n > \text{deg} D$, the isomorphism $\text{eval}_E : L(D) \rightarrow C$ will send this action to an action of G on C . Specifically, each $T \in G$ acts by sending $(f(P_1), f(P_2), \dots, f(P_n))$ to

$$\begin{aligned} &(T^*f(P_1), T^*f(P_2), \dots, T^*f(P_n)) \\ &= (f(T^{-1}(P_1)), f(T^{-1}(P_2)), \dots, f(T^{-1}(P_n))). \end{aligned}$$

If we also assume that G leaves E stable, then G acts by permutations on the set $\{P_1, \dots, P_n\}$. Thus $(T^{-1}(P_1), T^{-1}(P_2), \dots, T^{-1}(P_n))$ is a permutation of the points (P_1, P_2, \dots, P_n) , and the above action on C simply permutes the corresponding coordinates. The **permutation automorphism group** $\text{Perm} C$ of the code $C \subset F^n$ is the subgroup of S_n (acting on F^n by coordinate permutation) which preserves C .

Thus if $n > \text{deg} D$, there is a homomorphism from $\text{Aut}_{D,E}(X)$ to $\text{Perm} C$:

$$\begin{aligned} \rho : \text{Aut}_{D,E}(X) &\rightarrow \text{Perm} C, \\ T &\mapsto \text{eval}_E \circ T^* \circ \text{eval}_E^{-1}. \end{aligned}$$

In the next section, we will construct an inverse for this homomorphism.

IV. FROM CODE AUTOMORPHISMS TO CURVE AUTOMORPHISMS

Now we would like to answer the question: when does a group of permutation automorphisms of the code C induce a group of automorphisms of the curve X ? We will show that

permutation automorphisms of the code $C(D, E)$ induce curve automorphisms whenever D is very ample and the degree of E is large enough. Under these conditions, the groups $\text{Aut}_{D,E}(X)$ and $\text{Perm} C$ are isomorphic. In proving these facts, we generalize some results of Wesemeyer [14], who dealt with the planar case.

Theorem 1: Let X be an algebraic curve, D be a very ample divisor on X , and P_1, \dots, P_n be a set of points on X disjoint from the support of D . Let $E = P_1 + \dots + P_n$ be the associated divisor, and $C = C(D, E)$ the associated AG code. Let G be the group of permutation automorphisms of C . Then there is an integer $r \geq 1$ such that if $n > r \cdot \deg(D)$, then G can be lifted to a group of automorphisms of the curve X itself. This lifting defines a group homomorphism $\psi : \text{Perm} C \rightarrow \text{Aut}(X)$. Furthermore, the lifted automorphisms will preserve D and E , so the image of ψ will be contained in $\text{Aut}_{D,E}(X)$.

Remark 1: An explicit upper bound on r is determined in the proof of Corollary 3 below. The polynomials R_i below can be computed explicitly using Groebner bases using an elimination order, as described in §3.4 of [10] (note: r is the maximum of the $\deg(R_i)$, $i = 1, \dots, k$).

Proof: An outline of the proof is as follows. First, note that since $r \geq 1$, $n > \deg D$, so that $\text{eval}_E : L(D) \rightarrow C$ is a vector space isomorphism as in Section II. Thus the permutation action of G on C can be pulled back to a linear action on $L(D)$. Next, because D is very ample we can use the linear system $|D|$ to embed X into projective space $\mathbb{P}^d = \mathbb{P}(L(D))$, where $d = \dim L(D) - 1$. The vector space action of G on $L(D)$ induces a projective linear action on $\mathbb{P}(L(D))$. We will show that under the stated hypotheses, this action preserves the image of X in \mathbb{P}^d , so restricts to an action on X . Furthermore, this action will stabilize the divisors D and E .

To prove these claims, let us look more carefully at the action of G . Let τ be an element of $\text{Perm} C$; it acts by a permutation of the coordinates of a codeword in C , hence by permuting the points in the support of E . Specifically, τ acts as

$$(f(P_1), \dots, f(P_n)) \mapsto (f(P_{\tau(1)}), \dots, f(P_{\tau(n)})) \quad (3)$$

for every function $f \in L(D)$. Because the permutation action leaves the code C invariant, this image is also a codeword. Therefore, there is a function which we will call $\tau(f)$ in $L(D)$ such that

$$(f(P_{\tau(1)}), \dots, f(P_{\tau(n)})) = (\tau(f)(P_1), \dots, \tau(f)(P_n)). \quad (4)$$

This defines the action of G on $L(D)$. Note that the action thus defined is linear.

The linear action of G on $L(D)$ gives a projective linear action on $\mathbb{P}^d = \mathbb{P}(L(D))$. For concreteness, let us choose a basis f_0, \dots, f_d of $L(D)$ and let Y_0, \dots, Y_d denote a corresponding set of homogeneous coordinate functions on $\mathbb{P}^d = \mathbb{P}(L(D))$. Then if

$$\tau f_i = a_{0,i} f_0 + \dots + a_{d,i} f_d$$

then

$$\tau Y_i = a_{0,i} Y_0 + \dots + a_{d,i} Y_d.$$

(Recall $\text{Aut}(\mathbb{P}^d) = PGL(d+1)$; the $(d+1) \times (d+1)$ matrix associated to τ is $\{a_{i,j}\}$.) Indeed, this action of G defines an action of G on the homogeneous coordinate ring $F[Y_0, \dots, Y_d]$:

$$Y_0^{e_0} \dots Y_d^{e_d} \mapsto (\tau Y_0)^{e_0} \dots (\tau Y_d)^{e_d}. \quad (5)$$

Then the action on the projective space \mathbb{P}^d is as follows: an element τ of G will act on a point $Q = [Y_0 : \dots : Y_d]$ in \mathbb{P}^d via

$$\tau(Q) = \tau[Y_0 : \dots : Y_d] = [\tau^{-1} Y_0 : \dots : \tau^{-1} Y_d]. \quad (6)$$

As in Section III, we use τ^{-1} rather than τ here so that the action will be on the left.

In the coordinates we have chosen, the embedding $\phi : X \rightarrow \mathbb{P}^d$ is given by $Y_i = f_i(P)$, or

$$\phi : X \rightarrow \mathbb{P}^d,$$

$$P \mapsto [f_0(P) : \dots : f_d(P)].$$

Now that we have defined the embedding, we will show that the action of G on \mathbb{P}^d preserves $\phi(X)$, so restricts to an action on the curve, and that this curve action preserves D and E . We will start by showing that the action of G on \mathbb{P}^d preserves $\phi(E)$.

Consider the images of the points P_1, \dots, P_n of E . For each point P_i , its image $\phi(P_i)$ has projective coordinates $[Y_0 : \dots : Y_d] = [f_0(P_i) : \dots : f_d(P_i)]$. Then for any $\tau \in G$, we have

$$\begin{aligned} \tau^{-1}(\phi(P_i)) &= \tau^{-1}[Y_0 : \dots : Y_d] \\ &= [\tau f_0(P_i) : \dots : \tau f_d(P_i)] \\ &= [f_0(P_{\tau(i)}) : \dots : f_d(P_{\tau(i)})] \\ &= \phi(P_{\tau(i)}). \end{aligned} \quad (7)$$

Thus, a permutation of the code acts by the inverse permutation on the images of the points of E .

Now we will show that the image $\phi(X)$ is preserved by the action defined in (6) of G on \mathbb{P}^d . There is one trivial case: if $d = 1$, then X must have genus 0 and ϕ is an isomorphism, so the action on \mathbb{P}^1 is automatically an action on $\phi(X)$. For $d > 1$, the coordinates Y_i must satisfy some homogeneous polynomial relations defining $\phi(X)$. Let R_1, \dots, R_k denote a set of homogeneous polynomials of minimal degree that generate the ideal of $\phi(X)$ in \mathbb{P}^d , so that $\phi(X)$ is defined by $R_1(Y_0, \dots, Y_d) = 0, \dots, R_k(Y_0, \dots, Y_d) = 0$ and its homogeneous coordinate ring is

$$F[Y_0, \dots, Y_d]/(R_1, \dots, R_k).$$

Now let $\tau \in \text{Perm} C$ be an automorphism of the code, and consider the polynomials defining the image $\tau(\phi(X))$ of $\phi(X)$ under the induced action defined in (6) on \mathbb{P}^d . A point $Q \in \mathbb{P}^d$ is in $\tau(\phi(X))$ if and only if $\tau^{-1}Q$ is in $\phi(X)$, i.e. if and only if $R_i(\tau^{-1}Q) = 0$ for $i = 1, \dots, k$. But by the definition of the action of G on \mathbb{P}^d , this exactly means that $\tau R_i(Q) = 0$, where τR_i is defined as in (5). Thus the ideal of $\tau(\phi(X))$ is generated by $\tau(R_1), \dots, \tau(R_k)$. In order to show

that $\tau(\phi(X)) = \phi(X)$, we will show that the two ideals are the same.

Let r be the largest degree of the homogeneous polynomials R_i in the variables Y_j . The action τ defined in (5) is linear, so for each i , the degree of $\tau(R_i)$ will be the same as the degree of R_i . Therefore the largest degree of the polynomials $\tau(R_1), \dots, \tau(R_k)$ is also r . Consequently, if we pull $\tau(R_i)$ back to X by plugging in $Y_j = f_j$, the resulting rational function $\tau(R_i)(f_0, \dots, f_d)$ will be in $L(rD)$, for $1 \leq i \leq k$. Since R_i is in the ideal of $\phi(X)$, R_i vanishes at every point of X , including the points $\phi(P_1), \dots, \phi(P_n)$ in the image of E . Since, as we showed in (7), τ acts as a permutation of the points $\phi(P_i)$, $\tau(R_i)$ must also vanish on $\phi(P_1), \dots, \phi(P_n)$, so the pullback $\tau(R_i)(f_0, \dots, f_d)$ vanishes on E . This means that $\tau(R_i)(f_0, \dots, f_d)$ is in $L(rD - E)$. But if $n > r \cdot \deg(D)$, then $rD - E$ is a divisor of degree < 0 and $L(rD - E)$ is the trivial vector space, so $\tau(R_i)(f_0, \dots, f_d)$ must vanish identically on X . Thus $\tau(R_i)$ is in the vanishing ideal associated to $\phi(X)$, for each R_i and for every $\tau \in G$. This means that the ideal of $\tau(\phi(X))$ is contained in the ideal of $\phi(X)$; the same argument using τ^{-1} shows that the ideals must in fact be equal. Thus $\tau(\phi(X)) = \phi(X)$.

We have shown that the action of G on the code gives an action on $\phi(X)$, defined by (6), which we then pull back via the embedding to an action

$$\tau(P) = \phi^{-1}(\tau(\phi(P))). \quad (8)$$

on X . At each stage, the action was multiplicative, so we have a homomorphism $\psi : \text{Perm } C \rightarrow \text{Aut}(X)$. Using (7) it follows that E is invariant under this action; we now need to show that the action leaves D invariant. Consider an element τ of G and its action on D . Because the action τ defined in (8) on X was defined via the action in (4) on $L(D)$, we know that τ preserves $L(D)$. But suppose that τ did not preserve D itself, so that $\tau(D) = D'$, $D \neq D'$, but $L(D) = L(D')$. Then there must be a point P in the support of D such that its coefficient, d_P , in D is larger than its coefficient d'_P in D' . Now consider a function $f \in L(D)$. Because it is also in $L(D')$, we must have $\text{div}(f) + D' \geq 0$. Thus the coefficient of $\text{div}(f)$ at P must be at most d'_P . Thus $\text{div}(f) + D - (d_P - d'_P)P \geq 0$, so in particular f is in $L(D - P)$. This is true for any f in $L(D)$, so $L(D) = L(D - P)$. But we assumed that D was very ample; in particular $L(D)$ separates points, which means that $\dim L(D - P) = \dim L(D) - 1$, a contradiction. So the action of G on X must preserve D . This means that the image of the homomorphism $\psi : \text{Perm } C \rightarrow \text{Aut}(X)$ is in $\text{Aut}_{D,E}(X)$. \square

It should be clear from these constructions that ρ and ψ , when they exist, are inverses of each other, making $\text{Aut}_{D,E}(X)$ and $\text{Perm } C$ isomorphic groups.

Next we will find an explicit bound on the integer r in Theorem 1. Recall from the proof of Theorem 1 that r is bounded by the degrees of the polynomials R_1, \dots, R_k defining the embedding $\phi(X) \subset \mathbb{P}^d$. To bound these degrees, we use the following theorem of Gruson, Lazarsfeld, and Peskine.

Theorem 2 ([4]): Let $X \subseteq \mathbb{P}^d$ ($d \geq 3$) be a reduced irreducible curve of degree δ , not contained in any hyperplane,

over an algebraically closed field of arbitrary characteristic. Then the following property:

- X is cut out in \mathbb{P}^d by hypersurfaces of degree n , and the homogeneous ideal of X is generated in degrees $\geq n$ by its component of degree n .

holds for all $n \geq \delta + 2 - d$. It fails for $n = \delta + 1 - d$ if and only if X is a smooth rational curve having a $(\delta + 2 - d)$ -secant line.

In our case the degree δ of the embedded curve $\phi(X)$ is $\delta = \deg D$.

The result below is actually slightly stronger than the corresponding result of Wesemeyer (Corollary 4.9 [14]) for elliptic curves and elliptic codes.

Corollary 3: Let X be a smooth projective curve of genus $g \geq 2$. Let D be a divisor on X with $\deg D \geq 2g + 1$ and let E be the sum of at least $(1 + g) \deg D$ distinct points on X disjoint from the support of D . Then the group of permutation automorphisms of the code $C = C(D, E)$ is isomorphic to the group of automorphisms of X that fix both D and E .

Proof: Since $\deg D \geq 2g + 1$, D is very ample, so we use Theorem 1; we want to estimate r . Suppose that the image of the embedding $|D| : X \hookrightarrow \mathbb{P}^d$ defined over F is defined by multivariate polynomial relations $R_1 = 0, \dots, R_k = 0$ over F of minimal degree. As noted in the proof of Theorem 1, we can take r to be the maximal degree of the polynomials R_1, \dots, R_k . We will use Theorem 2 to do this.

We must show that $\phi(X)$ is not contained in any hyperplane. If it were, the equation for this hyperplane would define a linear relation among the coordinates Y_0, \dots, Y_d on $\phi(X)$. By the embedding equations $Y_i = f_i(P)$, this pulls back to a linear relation among f_0, \dots, f_d . But f_0, \dots, f_d form a basis of $L(D)$, so they are linearly independent. Therefore $\phi(X)$ cannot be contained in a hyperplane in \mathbb{P}^d ; furthermore $2 \leq r$.

We are working over a field F which is not necessarily algebraically closed. Given our divisor D over F , let \bar{D} be the associated divisor over the algebraic closure \bar{F} . By “base-change”, the image of the associated embedding $|\bar{D}| : X \hookrightarrow \mathbb{P}^d$ ($d = \dim L(D) - 1$) defined over \bar{F} is defined by the same multivariate polynomial relations $R_1 = 0, \dots, R_k = 0$ over F (and hence over \bar{F}). Therefore we can use Theorem 2 to estimate r , even though F may not be algebraically closed.

Following Theorem 2, then, we see that if $d \geq 3$, the maximum degree of the R_i 's is less than or equal to $\deg D + 1 - d$ in most cases, or $\deg D + 2 - d$ if X has genus zero and its image $\phi(X)$ is smooth and has a $\deg D + 2 - d$ -secant line. In our case, $d = \dim L(D) - 1$ and D is non-special, so by the Riemann-Roch theorem $d = \deg D - g$. Therefore if $g \geq 2$, we will have $d \geq 3$ and from [4], $r \leq 1 + g$. \square

There are a few special cases to consider that fall outside of Corollary 3. If X is rational, and $d = 1$, then the embedding is an isomorphism and the automorphism groups are the same. If $d = 2$, then the embedding is as a plane conic, so $r = 2$. For larger d , Theorem 2 holds and shows that $r = 2$ (and that X always has a 2-secant line, which is not surprising). In both of these cases, the groups are isomorphic if $\deg E \geq 2 \deg D$. If X has genus 1 and is embedded smoothly in \mathbb{P}^2 , it must be as a cubic so $r = \deg D = 3$; the groups will be isomorphic if $\deg E \geq 3 \deg D = 9$. Again, for larger d Theorem 2 holds

and shows that $r = 2$, so the groups are isomorphic if $\deg E \geq 2 \deg D$.

Remark 2: Under the hypotheses of Corollary 3, the length of C is $n = \deg E$, the dimension is $k = \deg D + 1 - g$, and the minimum distance $d \geq \deg E - \deg D$ (see for example Corollary II.2.3 [12]).

Remark 3: Let $F_0 \subset F$ denote a subfield of our finite field F and let $\Gamma = \text{Gal}(F/F_0)$ denote the Galois group (a cyclic group of order $[F : F_0]$). Let C be a linear code of length n over F with permutation automorphism group G . Consider the group $H = S_n \times \Gamma$, which acts on F^n via

$$h = (g, \sigma) : c = (c_1, \dots, c_n) \mapsto hc = (\sigma(c_{\tau(1)}), \dots, \sigma(c_{\tau(n)}).$$

This action is an isometry in the Hamming metric. The subgroup \overline{G} of H stabilizing C contains G . Our main result extends from G to \overline{G} .

V. EXAMPLES

Example 4: Let $F = GF(49)$ and let X denote the curve defined by

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

This has genus 3. The automorphism group $\text{Aut}_F(X)$ is a central 2-fold cover of $PGL_2(7)$: we have a short exact sequence,

$$1 \rightarrow H \rightarrow \text{Aut}_F(X) \rightarrow PGL_2(7) \rightarrow 1,$$

where H denotes the subgroup of $\text{Aut}_F(X)$ generated by the hyperelliptic involution (which happens to also be the center of $\text{Aut}_F(X)$). For details, see [2], Theorem 1.

Next, we recall some consequences of §3.2 in [9]. There are $|X(F)| = 2 \cdot 7^2 - 7 + 1 = 92$ F -rational points¹:

$$X(F) = \{P_1 = [1 : 0 : 1], P_2 = [0 : 0 : 1], \dots\}.$$

The automorphism group does not act transitively on $X(F)$ but has 2 orbits: the orbit C_1 of P_1 and the orbit $C_2 = X(F) - C_1$. We have $|C_1| = 7 + 1 = 8$ and $|C_2| = 2 \cdot 7 \cdot (7 - 1) = 84$.

Let $D = mP_1$, $E = X(F) - C_1 = \{Q_1, \dots, Q_{84}\}$, and let

$$C = C(D, E) = \{(f(Q_1), \dots, f(Q_{84})) \mid f \in L(D)\}.$$

This is an $[n, k, d]$ code over F , where $n = \deg(E) = 84$, $k \leq \dim(L(D))$.

Let $G = \text{Stab}(P_1, \text{Aut}_F(X))$ denote the stabilizer of P_1 . Since E is an orbit of the full automorphism group, it will also be stabilized by G , so $G = \text{Aut}_{D,E}(X)$. The group G is a non-abelian group of order $2 \cdot 7 \cdot (7 - 1) = 84$.

According to Corollary 3, $\text{Perm} C(D, E)$ will be isomorphic to G if we choose m so that $\deg D$ is at least $2g + 1 = 7$ and $\deg E = 84$ to be at least $(g + 1) \deg D = 4 \deg D$. Since $\deg D = m$, this means that $7 \leq m \leq 21$.

Assuming we choose $m > 2g - 2 = 4$, the Riemann-Roch theorem implies $\dim(L(D)) = m - 2$, so C is an $[84, m - 2, \geq$

¹We view the curve as embedded in a weighted projective space, with weights 1, 4, and 1, in which the point at infinity is nonsingular.

$84 - m]$ -code over $GF(49)$. Since G fixes D and preserves E , it acts on C via

$$g : (f(Q_1), \dots, f(Q_{84})) \mapsto (f(g^{-1}Q_1), \dots, f(g^{-1}Q_{84})),$$

for $g \in G$.

Remark 4: (a) More generally, for $p > 3$ and $p \equiv 3 \pmod{4}$, the curve X defined by $y^2 = x^p - x$ over $F = GF(p^2)$ is associated to an $[n = 2p(p - 1), k = \frac{p+5}{2}, d \geq 2p^2 - 3p - 1]$ code C . Using our results, it can be shown that C has permutation group isomorphic to the automorphism group of X , which is a 2-fold cover of $PGL_2(p)$ of size $2p(p^2 - 1)$. (Take $D = X(GF(p))$ and $E = X(GF(p^2)) - X(GF(p))$ in Proposition 3 of [7].) In [7], it is conjectured that C has a permutation decoding algorithm of complexity $O(n)$.

(b) Using the SAGE command `riemann_roch_space` (see the reference manual of SAGE [11] for more details on this command and the syntax), one can explicitly compute a basis of $L(D)$ in the examples given in this correspondence.

In some interesting cases, there are not enough rational points on the curve to apply Theorem 1.

Example 5: Again, let X denote the genus 3 curve defined by

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

but this time over $F = GF(7)$. The automorphism group $\text{Aut}_F(X)$ is now a central 2-fold cover of $PSL_2(7)$: we have a short exact sequence,

$$1 \rightarrow H \rightarrow \text{Aut}_F(X) \rightarrow PSL_2(7) \rightarrow 1, \quad (9)$$

where as before H denotes the subgroup of $\text{Aut}_F(X)$ generated by the hyperelliptic involution (which happens to also be the center of $\text{Aut}_F(X)$). The following transformations are generating elements of G :

$$\begin{aligned} \gamma_1 &= \begin{cases} x \mapsto x, \\ y \mapsto -y, \end{cases}, & \gamma_2 = \gamma_2(a) &= \begin{cases} x \mapsto a^2x, \\ y \mapsto ay, \end{cases} \\ \gamma_3 &= \begin{cases} x \mapsto x + 1, \\ y \mapsto y, \end{cases}, & \gamma_4 &= \begin{cases} x \mapsto -1/x, \\ y \mapsto y/x^4, \end{cases} \end{aligned} \quad (10)$$

where $a \in F^\times$ is a primitive 6-*th* root of unity (for (10), see [2]; (9) was verified using [1]).

On this curve there are only 8 F -rational points:

$$\begin{aligned} X(F) &= \{P_1 = [1 : 0 : 0], P_2 = [0 : 0 : 1], \\ &P_3 = [1 : 0 : 1], \dots, P_8 = [6 : 0 : 1]\}. \end{aligned}$$

Thus it is impossible to choose D and E so that $\deg D \geq 7$ and E consists of at least 4 $\deg D$ distinct rational points. Let us instead choose $D = mP_1$ and E to be all of the other rational points as before, and compare $\text{Perm} C$ and $\text{Aut}_{D,E}(X)$.

The automorphism group acts transitively on $X(F)$; as in the previous example let $G = \text{Aut}_{D,E}(X) = \text{Stab}(P_1, \text{Aut}_F(X))$, the stabilizer of the point at infinity in $X(F)$. (All of the stabilizers $\text{Stab}(P_i, \text{Aut}_F(X))$ are conjugate to each other in $\text{Aut}_F(X)$, $1 \leq i \leq 8$). The group G is a non-abelian group of order 42. (In fact, the group $G/Z(G)$

is the non-abelian group of order 21, where $Z(G)$ denotes the center of G .) Take the automorphisms γ_1, γ_2 with $a = 2$ and γ_3 as generators of G . If we identify $S = \{P_2, \dots, P_8\}$ with $\{1, 2, \dots, 7\}$ then

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

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

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

Let $D = 5P_1$, $S = C(F) - \{P_1\}$, and let

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

This is a $[7, 3, 5]$ code over F . In fact, $\dim(L(D)) = 3$, so the evaluation map $f \mapsto (f(P_2), \dots, f(P_8))$, $f \in L(D)$, is injective. Since G fixes D and preserves E , it acts on C via

$$g : (f(P_2), \dots, f(P_8)) \mapsto (f(g^{-1}P_2), \dots, f(g^{-1}P_8)),$$

for $g \in G$.

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

$$\rho : G \rightarrow P.$$

What is the kernel of this map? There are two possibilities: either a subgroup of order 6 or a subgroup of order 21. (This is obtained using [1] by matching possible orders of quotients G/N with possible orders of subgroups of P). Indeed, the kernel $\ker(\phi) = N = \langle g_2, g_3 \rangle$ is a non-abelian normal subgroup of $G = \langle g_1, g_2, g_3 \rangle$ of order 21.

ACKNOWLEDGEMENT

We thank Jessica Sidman for the reference in the proof of Corollary 3 and Will Traves for many helpful conversations. We also thank the referees for many helpful comments, in particular for prompting us to clarify the proof of Theorem 1.

REFERENCES

- [1] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4*; 2005. Available: <http://www.gap-system.org>
- [2] N. Göb, “Computing the automorphism groups of hyperelliptic function fields,” preprint, 2003. Available: <http://front.math.ucdavis.edu/math.NT/0305284>
- [3] V. D. Goppa, *Geometry and Codes*. Hingham, MA: Kluwer Academic Publishers, 1988.
- [4] L. Gruson, R. Lazarsfeld, and C. Peskine, “On a theorem of Castelnuovo, and the equations defining space curves,” *Invent. Math.*, vol.72, no. 3, pp. 491-506, 1983.
- [5] D. Joyner, “GUAVA: An error-correcting codes package,” *SIGSAM Comm. Computer Algebra*, vol. 39, no. 2, pp. 65-68, 2005. Available: <http://www.gap-system.org/Packages/guava.html>
- [6] C. Heegard, J. Little, K. Saints, “Systematic encoding via Gröbner bases for a class of algebraic-geometric Goppa codes,” *IEEE Trans. Info. Theory*, vol. 41, pp. 1752-1761, Nov. 1995.
- [7] D. Joyner, “Conjectural permutation decoding of some AG codes,” *SIGSAM Comm. Computer Algebra*, vol. 39, no. 1, pp. 166-172, 2005.
- [8] — and A. Ksir, “Decomposing representations of finite groups on Riemann-Roch spaces,” to be published in *Proc. Amer. Math. Soc.*

- [9] — and W. Traves, “Representations of finite groups on Riemann-Roch spaces,” preprint, 2004. Available: <http://front.math.ucdavis.edu/math.AG/0210408>
- [10] M. Kreuzer and L. Robbiano, *Computational Commutative Algebra, I*. New York: Springer-Verlag, 2000.
- [11] W. Stein and D. Joyner, “SAGE: System for Algebra and Geometry Experimentation,” *SIGSAM Comm. Computer Algebra*, vol. 39, no. 2, pp. 61-64, 2005. Available: <http://sage.scipy.org/>, <http://sage.sf.net/>
- [12] H. Stichtenoth, *Algebraic Function Fields and Codes*. New York: Springer-Verlag, 1993.
- [13] M.A. Tsfasman and S.G. Vlăduț, *Algebraic-geometric Codes*. Hingham, MA: Kluwer Academic Publishers, 1991.
- [14] S. Wesemeyer, “On the automorphism group of various Goppa codes,” *IEEE Trans. Info. Theory*, vol. 44, pp. 630-643, Mar. 1998.

David Joyner David Joyner received his BS in Mathematics from the Georgia Institute of Technology in 1981 and his PhD in Mathematics from the University of Maryland College Park in 1983. He was an NSF Fellow from 1984-1987 and has been at the United States Naval Academy, where he is now a professor in the Mathematics Department, since 1987. He is the maintainer of the error-correcting codes computer algebra package GUAVA and has published research papers in coding theory, representation theory, and automorphic forms.

Amy Ksir Amy Ksir received her BA in Mathematics from Rice University in 1993 and her PhD in Mathematics from the University of Pennsylvania in 1999. She has been at the United States Naval Academy as an assistant professor in the Mathematics Department since 2003. She has published research papers in algebraic geometry, coding theory, and string theory.