Automorphism groups of some AG codes

David Joyner and Amy Ksir*

12-9-2004

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 [W] beyond the case of planar curves.

1 Introduction

The construction of AG codes uses the Riemann-Roch space $L(D)$ associated to a divisor D of a curve X defined over a finite field [G]. 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 paper we show that, in some cases, the automorphism group of a curve and the permutation automorphism group of a corresponding AG code are in fact the same.

We thank Jessica Sidman for the reference in the proof of Corollary 3 and Will Traves for many helpful conversations.

*Mathematics Dept, USNA, Annapolis, MD 21402, wdj@usna.edu and ksir@usna.edu

2 The Riemann-Roch space $L(D)$ and the associated AG code.

Let X be a smooth projective curve 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

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

where $div(f)$ denotes the (principal) divisor of the function $f \in F(X)$. It is well-known that these have an F-rational vector space structure [Sti], [TV]. More precisely, if $\bar{D}$ denotes the corresponding divisor over the algebraic closure $\bar{F}$, then $L(\bar{D}) = L(D) \otimes \bar{F}$.

Let $P_1, ..., P_n \in X(F)$ be distinct points, and let $E = P_1 + \ldots + P_n$ 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

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

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

$$\begin{aligned} eval_E : L(D) &\to F^n, \\ f &\longmapsto (f(P_1), \ldots, f(P_n)). \end{aligned} \tag{2}$$

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

3 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. Then G also acts on the code C, as follows.

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

$$\begin{array}{rccc} \rho : & \mathrm{Aut}(X) & \longrightarrow & \mathrm{Aut}(F(X)), \\ & g & \longmapsto & (f \longmapsto f^g) \end{array}$$

where for any $P \in X$, $f^g(P) = (\rho(g)(f))(P) = f(g^{-1}(P))$.

Note that $Y = X/G$ is also smooth and $F(X)^G = F(Y)$.

Of course, $\mathrm{Aut}(X)$ also acts on the group $Div(X)$ of divisors of X, denoted $g(\sum_P d_P P) = \sum_P d_P g(P)$, for $g \in \mathrm{Aut(X)}$, P a prime divisor, and $d_P \in \mathbb{Z}$. It is easy to show that $div(f^g) = g(div(f))$. Because of this, if $div(f) + D \geq 0$ then $div(f^g) + g(D) \geq 0$, for all $g \in \mathrm{Aut}(X)$. In particular, if the action of $G \subset \mathrm{Aut}(X)$ on X leaves $D \in Div(X)$ stable then G also acts on $L(D)$. We denote this action by

$$\rho : G \to \mathrm{Aut}(L(D)).$$

Assuming that $n > \deg D$, the isomorphism $eval_E : L(D) \to C$ will send this action to an action of G on C. Specifically, each $g \in G$ acts by

$$\begin{aligned}(f(P_1), f(P_2), \ldots f(P_n)) &\mapsto (f^g(P_1), f^g(P_2), \ldots, f^g(P_n)) \\ &= (f(g^{-1}(P_1)), f(g^{-1}(P_2)), \ldots f(g^{-1}(P_n))).\end{aligned}$$

If we also assume that G leaves E stable, then G acts by permutations on the set $\{P_1, \ldots, P_n\}$. Thus $(g^{-1}(P_1), g^{-1}(P_2), \ldots, g^{-1}(P_n))$ is a permutation of the points $(P_1, P_2, \ldots, P_n)$, and the above action on C simply permutes the corresponding coordinates.

Definition 1 *The* **permutation automorphism group** *of the code $C \subset F^n$ is the subgroup of S_n (acting on F^n by coordinate permutation) which preserves C.*

4 From code automorphisms to curve automorphisms.

Now we would like to answer the question: when does a group of automorphisms of the code C induce a group of automorphisms of the curve X? We will show that automorphisms of the code $C(D, E)$ induce curve automorphisms whenever D is very ample and the degree of E is large enough. In proving these facts, we generalize some results of Wesemeyer [W], who dealt with the planar case.

Theorem 2 *Let X be an algebraic curve, D be a very ample divisor on X, and $P_1 \ldots P_n$ be a set of points on X disjoint from the support of D. Let*

$E = P_1 + \ldots + P_n$ 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.

proof: First, note that since $n > \deg D$, $eval_E : L(D) \to C$ is a vector space isomorphism. Thus the action of G on C can be pulled back to an action on $L(D)$. Next, we use D to embed X into projective space $\mathbb{P}^d$, where $d = \dim L(D) - 1$. If we let $Y_0, \ldots, Y_d$ be a basis for $L(D)$, then the embedding is given explicitly by

$$\phi : X \to \mathbb{P}^d,$$
$$P \longmapsto [Y_0(P) : \ \ldots \ : Y_d(P)].$$

The vector space action of G on $L(D)$ induces an action on the polynomial ring $F[Y_0, \ldots Y_d]$ and a projective linear action on $\mathbb{P}^d$. The question now is whether this action preserves the image of X in $\mathbb{P}^d$.

The coordinates Y_i obviously satisfy some homogeneous polynomial relations defining the image of X. Let $R_1(Y_0, \ldots, Y_d) = 0, \ldots, R_k(Y_0, \ldots, Y_d) = 0$ denote a set of polynomials of minimal degree that define the ideal of X in $\mathbb{P}^d$, so that its projective coordinate ring is

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

Since $R_1, \ldots, R_k$ are polynomials in $Y_0, \ldots, Y_d$, and $Y_0, \ldots, Y_d$ are in $L(D)$, the $R_1, \ldots, R_k$ will be in $L(rD)$ for some $r \geq 1$. In particular if we let r be the largest degree of the R_i's in the Y_j's, then each R_i will be in $L(rD)$. (Often this is true for a smaller r, in fact).

Now let $T \in G$ be an automorphism of the code, and consider the image $T(X)$ of X under the induced action on $\mathbb{P}^d$. The ideal of $T(X)$ is generated by $T(R_1), \ldots, T(R_k)$, where $T(R_i)(Y_0, \ldots Y_d) = R_i(T(Y_0), \ldots, T(Y_d))$. If we can show that these functions are also in the ideal of X, for any $T \in G$, then the ideals will be equal and we will have given an action of G on X, as desired.

Let $R_i \in L(rD)$ be one of the minimal degree generators of the ideal of X. Since $R_i \in L(rD)$ and R_i is in the ideal of X, R_i vanishes at every point of X, including $P_1, \ldots, P_n$. Since D and E are both stable under the action of G, $T(R_i)$ will also be in $L(rD)$, and will also vanish at E. This means that $T(R_i)$ 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 $T(R_i)$ must vanish identically on X. Thus $T(R_i)$ is in the vanishing ideal associated to X, for each R_i and for every $T \in G$. $\square$

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

Corollary 3 *Let X be a smooth projective curve of genus $g > 0$. Let D be a divisor on X with degree $2g + 1 < \deg D$ and let E be a collection of at least $(1 + g) \deg D$ 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: Assume for the moment that F is algebraically closed. If the image of X is not contained in any hyperplane in $\mathbb{P}^d$, then Gruson, Lazarsfeld, and Peskine [GLP] (since F is algebraically closed) give the maximum degree of the $R_i's$ as $\deg D + 1 - d$ in most cases, or $\deg D + 2 - d$ if X has genus zero and its image is smooth and has a $\deg D + 2 - d$-secant line. In our case, where $d = \dim L(D) - 1$ and D is non-special, this means that $r \leq 1 + g$, if the genus g of X is greater than zero, and $r \leq 2$ if X is rational and there is a line in $\mathbb{P}^d$ which intersects X in two points.

Now we indicate how the hypothesis that F is algebraically closed may be removed. Suppose that the image of an embedding $X \hookrightarrow \mathbb{P}^{\deg D}$ defined over F is defined by multivariate polynomial relations $R_1 = 0$, ..., $R_k = 0$ over F. By "base-change", we see that the image of the associated embedding $X \hookrightarrow \mathbb{P}^{\deg D}$ defined over $\overline{F}$ is defined by the same multivariate polynomial relations $R_1 = 0$, ..., $R_k = 0$ over F (and hence over $\overline{F}$). This observation is all that is needed to show that the bound on the degrees of the R_i's in the non-algebraically closed case. $\square$

Remark 1 *The length of C is $n = \deg E$, dimension is $k = \deg D + 1 - g$, and minimum distance $d \geq \deg E - \deg D$ (see for example Corollary II.2.3 [Sti]).*

Example 4 *The bounds in the hypotheses to the above Corollary are not sharp. For example, let $F = GF(49)$ and let X denote the curve defined by*

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

This has genus 3. The automorphism group $Aut_F(X)$ is a central 2-fold cover of $PGL_2(F)$: we have a short exact sequence,

$$1 \to H \to Aut_F(X) \to PGL_2(7) \to 1,$$

where H denotes the subgroup of $Aut_F(X)$ generated by the hyperelliptic involution (which happens to also be the center of $Aut_F(X)$). For details, see [G], Theorem 1.

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

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

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 $G = Stab(P_1, Aut_F(X))$ denote the stabilizer of P_1. The group G is a non-abelian group of order $2 \cdot 7 \cdot (7-1) = 84$

It is known (Proposition VI.4.1, [Sti]) 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 $D = mP_1$, $E = X(F) - C_1 = \{Q_1, \ldots, Q_{84}\}$, and let

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

This is a $[n, k, d]$ code over F, where $n = deg(E) = 84$, $k \leq dim(L(D))$. If $m > 2g - 2 = 4$ then the Riemann-Roch theorem implies $dim(L(D)) = m - 2$, so C is an $[84, m-2, \geq 84 - m]$-code over $GF(49)$. In fact, if the evaluation map $f \longmapsto (f(Q_1), \ldots, f(Q_{84}))$, $f \in L(D)$, is injective then $k = dim(L(D))$. Since G fixes D and preserves S, it acts on C via

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

for $g \in G$.

Let P denote the permutation group of this code. Taking $r = 1$ in Theorem 2, we see that if $4 < m < n = 84$ then $P = G$. According to the Corollary, if $m > 7$ and $n > 4m$ then $P = G$. Therefore the bounds in the above Corollary are not sharp.

[1] MAGMA views the curve as embedded in a weighted projective space, with weights 1, 4, and 1, in which the point at infinity is nonsingular.

Next, a non-example to show that the hypothesis that $X(F)$ has "sufficiently many points" cannot be dropped.

Example 5 *Let $F = GF(7)$ and let X denote the curve defined by*

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

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

$$1 \to H \to Aut_F(X) \to PSL_2(7) \to 1,$$

where H denotes the subgroup of $Aut_F(X)$ generated by the hyperelliptic involution (which happens to also be the center of $Aut_F(X)$).

There are 8 F-rational points:

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

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

Let $G = Stab(P_1, Aut_F(X))$ denote the stabilizer of the point at infinity in $X(F)$. All the stabilizers $Stab(P_i, Aut_F(X))$ are conjugate to each other in $Aut_F(X)$, $1 \le i \le 8$. 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.)

It is known (Proposition VI.4.1, [Sti]) that, for each $m \ge 1$, the Riemann-Roch space $L(mP_1)$ has a basis consisting of monomials,

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

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

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

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

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

for $g \in G$.

Let P *denote the permutation group of this code. It 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*

$$\psi : G \to P.$$

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 by matching possible orders of quotients* G/N *with possible orders of subgroups of* P*). Take the automorphisms* γ_1, γ_2 *with* $a = 2$ *and* γ_3. *If we identify* $S = \{P_2, \ldots, P_8\}$ *with* $\{1, 2, \ldots, 7\}$ *then*

$$\gamma_1 \leftrightarrow (2,7)(3,6)(4,5) = g_1,$$
$$\gamma_2 \leftrightarrow (2,5,3)(4,6,7) = g_2,$$
$$\gamma_3 \leftrightarrow (1,2,\ldots 7) = g_3.$$

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

References

[G] V. D. Goppa, **Geometry and codes**, Kluwer, 1988.

[GLP] L. Gruson, R. Lazarsfeld, and C. Peskine, "On a Theorem of Castelnuovo, and the Equations Defining Space Curves," *Invent. math.* **72**, 491-506 (1983).

[JK] D. Joyner and A. Ksir, "Representations of finite groups on Riemann-Roch spaces, II," preprint 2003, available at `http://front.math.ucdavis.edu/math.AG/0312383`

[JT] D. Joyner and W. Traves, "Representations of finite groups on Riemann-Roch spaces," preprint, 2002 available at `http://front.math.ucdavis.edu/math.AG/0210408` (revised version posted April, 2004)

[MAGMA] W. Bosma, J. Cannon, C. Playoust, "The MAGMA algebra system, I: The user language," J. Symb. Comp., 24(1997)235-265. (See also the MAGMA homepage at `http://www.maths.usyd.edu.au:8000/u/magma/`).

[Sti] H. Stichtenoth, **Algebraic function fields and codes**, Springer-Verlag, 1993.

[TV] M.A. Tsfasman and S.G. Vlädut, **Algebraic-Geometric Codes**, Kluwer Academic Publishers, 1991.

[W] S. Wesemeyer, "On the Automorphism Group of Various Goppa Codes," IEEE Trans. Info. Theory., 44(1998)630-643.