Modular representations on Riemann-Roch spaces: computational aspects

David Joyner, Math Dept, USNA*

Contents

1 Introduction **2**
1.1 History . . . 3
1.2 The results . . . 3
1.3 The action of G on $L(D)$ . . . 4

2 Easy cases **4**
2.1 Toric varieties . . . 5
2.2 The projective line . . . 9

3 Algorithms in the hyperelliptic curve case **11**
3.1 Computing G-equivariant divisors . . . 11
3.2 The decomposition of the Riemann-Roch space . . . 12

4 The general curve case **13**
4.1 Bounds on the size of the irreducible submodules of $L(D)$ . . . 13
4.2 Borne's formula . . . 14
4.2.1 Computing the ramification module . . . 15
4.2.2 A formula for the multiplicity . . . 16
4.3 Examples: good characteristic . . . 17
4.4 Examples: bad characteristic . . . 25
4.4.1 General remarks . . . 25
4.4.2 Examples . . . 29

*Notes for talk at Clemson Univ, 10-23-2003. Revised 5-28-2005.

5 Appendix: Representation-theoretic background **36**

6 Appendix: MAGMA code **38**

This talk surveys without proofs some of the authors' recent work on computing modular representations on Riemann-Roch spaces. Most of this is joint work with Amy Ksir [JK] (sections 4.2 and beyond) and Will Traves [JT] (§4.1 and parts of §2.2). This work was partially supported by an NSA-MSP grant.

Ackowledgements: Many thanks to Thomas Brauer and Frank Luebeck of GAP along with Claus Fieker and David Kohel of MAGMA for helpful emails.

1 Introduction

Some questions concerning automorphism groups of Goppa codes lead to the following situation.

Let X be a smooth projective variety over an algebraically closed field F and let G be a finite subgroup of automorphisms of X over F. Let us, when convenient, identify X with its set of F-rational points $X(F)$. If D is a divisor of X which G leaves stable then G acts on the Riemann-Roch space $L(D) = H^0(X, \mathcal{O}(D))$. Several natural questions arise. For example:

1. Does *any* representation of G arise as an irreducible subrepresentation of $L(D)$ for some such D?

2. Is there an explicitly computable formula for the multiplicity of a given irreducible representation of G in $L(D)$?

Note that this last question is tantamount to asking for a formula for the trace of the representation of G on $L(D)$. Such a formula would generalize the Eichler trace formula.

1.1 History

The action of G on the space of regular differentials, $\Omega^1(X)$ (which is isomorphic to $L(K)$, where K is a canonical divisor) was looked at from the representation-theoretic point-of-view by Hurwitz (G cyclic), Weil and Chevalley (any G). They were studying monodromy representations on compact Riemann surfaces. Eichler computed the trace of the matrix representation of a g acting on $\Omega^1(X)$.

Later, Ellingsrud, Lonsted, Nakajima, Köck, Borne, Kani and others[1] looked at the action of G on $H^i(X, \mathcal{F})$, where $\mathcal{F}$ is a "G-sheaf" on X. They determined that the answer to question 1 is yes, at least if the characteristic of F is "good". They also answered question 2, at least for fields of good characteristic and divisors of "large degree", depending on your definition of "explicitly computable". Our form is different and based on a different method.

1.2 The results

The results include the following.

1. The analogous questions for toric varieties can be answered completely.

2. In the case when the characteristic of F is relatively prime to $|G|$, the natural representation of G on $L(D)$ is a direct sum of irreducible representations of dimension $\leq d$, where d is the size of the smallest G-orbit in X. W There are examples in genus 0 which show that this is sharp (i.e., that dimension d subrepresentations do occur).

3. Suppose that F has characteristic 0 and let ρ denote an irreducible $\mathbb{Q}[G]$-module. If D is a non-special G-equivariant divisor and if $L(D)$ has a $\mathbb{Q}[G]$-module structure then we find a formula for the multiplicity of ρ in $L(D)$. We (AK+DJ) ave results which are more general than this. However, the statement is rather technical and, in any case, does not cover the situation wher e

4. If F has characteristic p and p divides $|G|$ then we have no general results. However, the code in §6 and the examples in §4.4 may be illuminating.

[1] See Borne [Bo], [Br], and [JT] for more references and history.

1.3 The action of G on $L(D)$

Let X be a smooth projective curve over an algebraically closed field F. Let $F(X)$ denote the function field of X (the field of rational functions on X) and, if D is any divisor on X then the **Riemann-Roch space** $L(D)$ is a finite dimensional F-vector space given by

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

where $div(f)$ denotes the (principal) divisor of the function $f \in F(X)$. Let $\ell(D)$ denote its dimension.

We recall the **Riemann-Roch theorem**,

$$\ell(D) - \ell(K - D) = \deg(D) + 1 - g,$$

where K denotes a canonical divisor and g the genus.

Denote the space of all Weil differentials by $\Omega(X)$. Since G acts on the set of places of F, it acts on the "adele ring" of F, hence on the space $\Omega(X)$. This action restricts to an action on the regular differentials, $\Omega^1(X)$.

The action of $\mathrm{Aut}(X)$ on $F(X)$

$$\rho : \mathrm{Aut}(X) \longrightarrow \mathrm{Aut}(F(X)),$$

is defined by $(\rho(g)(f))(x) = f(g^{-1}(x))$.

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 $g \in \mathrm{Aut}(X)$ and $d_P \in \mathbb{Z}$. It is easy to show that $div(\rho(g)f) = g(div(f))$. Because of this, if $div(f) + D \geq 0$ then $div(\rho(g)f) + g(D) \geq 0$, for all $g \in \mathrm{Aut}(X)$.

If the action of $G \subset \mathrm{Aut}(X)$ on X leaves $D \in Div(X)$ stable then we denote the associated representation of G in $L(D)$ by ρ:

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

2 Easy cases

The discussion of the question of which representations ρ arise is relatively simple in the cases of (toric automorphisms of) toric varieties and projective lines.

2.1 Toric varieties

Assume F is algebraically closed of characteristic 0. We first give a brief and incomplete sketch of some constructions related to toric varieties. For details, see for example Fulton [F].

Let $R = F[x_1, ..., x_n]$ be a ring in n variables. A **binomial relation** in R is one of the form

$$x_1^{k_1} ... x_n^{k_n} = x_1^{\ell_1} ... x_n^{\ell_n},$$

where $k_i \geq 0$, $\ell_j \geq 0$ are integers. A **binomial variety** is a subvariety of complex affine n-space $\mathbb{A}_F^n$ defined by a finite set of binomial equations. A typical "toric variety" is binomial, though they will be introduced via a combinatorial-geometry construction. The rough idea behind constructing a toric variety is to replace each such binomial equation as above by a relation in a semigroup S contained in a lattice L and replace R by the "group algebra" of this semigroup.

Associate to the dual cone σ^* the semigroup

$$S_\sigma = \sigma^* \cap L^* = \{w \in L^* \mid \langle v, w \rangle \geq 0, \ \forall v \in \sigma\}.$$

If $u_1, \ldots u_t \in L^*$ are semigroup generators of S_σ then we write $S_\sigma = \mathbb{Z}_{\geq 0}[u_1, ..., u_t]$, for brevity. Let $R_\sigma = F[S_\sigma]$ denote the "group algebra" of this semigroup and let

$$U_\sigma = \text{Spec } R_\sigma.$$

This defines an **affine toric variety** (associated to σ).

Let $\mathbb{G}_m$ denote the multiplicative algebraic group over F. For each integer k, the map $z \longmapsto z^k$ defines an element of $\text{Hom}_{alg.gp.}(\mathbb{G}_m, \mathbb{G}_m)$. Let $T = T_L = \text{Hom}_{ab.gp.}(L^*, \mathbb{G}_m)$. It is easy to show that $T \subset U_\sigma$. They have the same dimension, so T must be dense in U_σ.

Definition 1. *A* **fan** *in a lattice L is a set $\Delta = \{\sigma\}$ of rational strongly convex polyhedral cones in $L_\mathbb{Q} = L \otimes \mathbb{Q}$ such that*

- *if $\sigma \in \Delta$ and $\tau \subset \sigma$ is a face of σ then $\tau \in \Delta$,*
- *if $\sigma_1, \sigma_2 \in \Delta$ then $\sigma_1 \cap \sigma_2$ is a face of both σ_1 and σ_2 (and hence belongs to Δ by the above).*

If $L_\mathbb{Q} = \cup_{\sigma \in \Delta} \sigma$ then we call the fan **complete**.

We shall assume that all fans are finite.

Patching these affine toric varieties together for each σ in a fan Δ gives the **toric variety**

$$X(\Delta) = \cup_{\sigma \in \Delta} U_\sigma.$$

(It is not always projective but is always birational to $\mathbb{P}^m$, for some m.) Note that since T is dense in each affine patch, it must be dense in $X(\Delta)$.

Let Δ be a fan (a simplicial complex) in a lattice L. Denote by τ_1, ..., τ_n the edges or rays of the fan and let v_i denote the first (smallest) lattice point along the ray τ_i. Let D_i denote the Weil divisor

$$D_i = \mathrm{Hom}(\tau_i^* \cap L^*, F^\times),$$

(* denotes dual) which maybe regarded as the closure of the orbit of T acting on the edge τ_i.

If $X(\Delta)$ is complete and $D = d_1 + ... + d_n D_n$ then it is known that the Riemann-Roch space is generated by an explicit set of monomials:

$$L(D) = \oplus_{m \in P_D \cap L} F \cdot x^m,$$

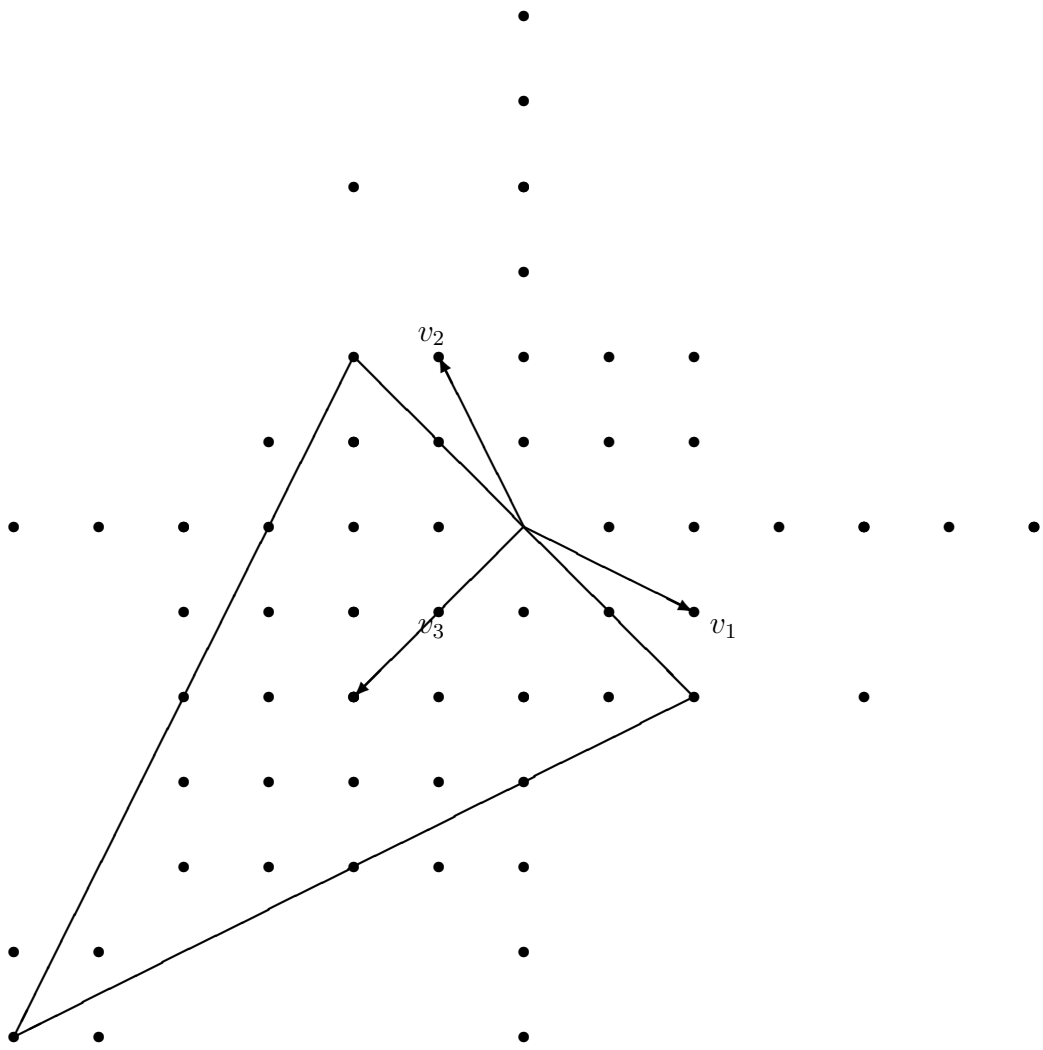
using multi-index notation, where x_i are local coordinates.

The **toric** package, written in GAP and MAGMA, computes these coordinate rings R_σ, Riemann-Roch spaces $L(D)$'s (and much more) [J1], [JV].

Example 2. *Let Δ be the fan generated by*

$$v_1 = 2e_1 - e_2, \quad v_2 = -e_1 + 2e_2, \quad v_3 = -e_1 - e_2.$$

In the notation above, the divisor $D = d_1 D_1 + d_2 D_2 + d_3 D_3$ is a Cartier divisor if and only if $d_1 \equiv d_2 \equiv d_3 \pmod 3$.



Let G denote the automorphism group of Δ generated by the map g sending (x, y) to (y, x), swapping v_1 and v_2 and leaving v_3 fixed. This corresponds to a T-equivariant automorphism of $X(\Delta)$.

Let

$$\begin{aligned} P_D &= \{(x, y) \mid \langle (x, y), v_i \rangle \geq -d_i,\ \forall i\} \\ &= \{(x, y) \mid 2x - y \geq -d_1, -x + 2y \geq -d_2, -x - y \geq -d_3\} \end{aligned}$$

denote the polytope associated to the Weil divisor $D = d_1 D_1 + d_2 D_2 + d_3 D_3$,

where D_i is as above.

Let $d_1 = d_2 = 6$ and $d_3 = 0$. Then P_D is a triangle in the plane with vertices at $(-6,-6)$, $(-2,2)$, and $(2,-2)$. Note that it remains invariant under the action of G. Moreover, the G action on $P_D \cap L^*$ has 7 singleton orbits (the lattice points $(-i,-i)$, where $0 \leq i \leq 6$) and 12 orbits of size 2.

In this example, the patch U_{σ_1} is an affine variety with coordinates x_1, x_2, x_3 given by $x_1^3 - x_2x_3 = 0$. The automorphism g acts on U_{σ_1} sending (x_1, x_2, x_3) to (x_1, x_3, x_2). The torus embedding $T \hookrightarrow U_{\sigma_1}$ is given by sending (t_1, t_2) to $(x_1, x_2, x_3) = (t_1t_2, t_1t_2^2, t_1^2t_2)$.

The patch U_{σ_2} is an affine variety with coordinates y_1, y_2, y_3 given by $y_1^2 - y_1y_3 = 0$. The automorphism g does not act on U_{σ_2}. The torus embedding $T \hookrightarrow U_{\sigma_2}$ is given by sending (t_1, t_2) to $(y_1, y_2, y_3) = (t_1^{-2}t_2^{-1}, t_1^{-1}, t_1^{-1}t_2)$.

The patch U_{σ_3} is an affine variety with coordinates z_1, z_2, z_3 given by $z_1^2 - z_1z_3 = 0$. The automorphism g does not act on U_{σ_3}. The torus embedding $T \hookrightarrow U_{\sigma_3}$ is given by sending (t_1, t_2) to $(x_1, x_2, x_3) = (t_1^{-1}t_2^{-2}, t_2^{-1}, t_1t_2^{-1})$. The automorphism g sends U_{σ_2} to U_{σ_3} by sending (y_1, y_2, y_3) to (z_1, z_2, z_3). In this case, we know

$$L(D) = \oplus_{m \in P_D \cap \mathbb{Z}^2} F \cdot x^m,$$

where x_1 and x_2 are local coordinates. The action of G on $L(D)$ is via its action on P_D.

Let Δ be a fan associated to an integral lattice L in $\mathbb{R}^n$. Let P_D denote the polytope associated to the Weil divisor D on $X = X(\Delta)$.

Theorem 3. *Let $X = X(\Delta)$ be a complete toric variety defined over an algebraically closed field F of characteristic 0. Suppose $G \subset \mathrm{Aut}_T(X)$ (= the toric automorphism group of X) is a finite subgroup and that the T-invariant Weil divisor D on X is fixed by G. Let P_D denote the polytope associated to D and let $S = P_D \cap L^*$. Let*

$$S = S_1 \cup S_2 \cup ... \cup S_k$$

denote the decomposition of S into disjoint primitive G-sets (orbits). For each $m \geq 1$, the natural representation π of G on $L(D)$ decomposes into a direct sum of k irreducible permutation representations

$$\pi = \oplus_{i=1}^k \pi_i,$$

where π_i is $|S_i|$-dimensional.

Corollary 4. *In the notation of the theorem above, the trace of $\pi(g)$ is the number of fixed points of g on S.*

For details, see [J2].

2.2 The projective line

Let $X = \mathbb{P}^1/F$, so $\mathrm{Aut}(X) = PGL(2, F)$, where F is algebraically closed. Let $\infty \in X$ denote the element corresponding to the localization $F[x]_{(1/x)}$.

A basis for the Riemann-Roch space is explicitly known for $\mathbb{P}^1$. For notational simplicity, let

$$m_P(x) = \begin{cases} x, & P = [1:0] = \infty, \\ (x-p)^{-1}, & P = [p:1]. \end{cases}$$

I don't know of a single reference for the following result but it is not hard to prove.

Lemma 5. *Let $P_0 = \infty = [1:0] \in X$ denote the point corresponding to the localization $F[x]_{(1/x)}$. For $1 \le i \le s$, let $P_i = [p_i : 1]$ denote the point corresponding to the localization $F[x]_{(x-p_i)}$, for $p_i \in F$. Let $D = \sum_{i=0}^{s} a_i P_i$ be a divisor, $a_k \in \mathbb{Z}$ for $0 \le k \le s$.*

(a) If D is effective then

$$\{1, m_{P_i}(x)^k \mid 1 \le k \le a_i, 0 \le i \le s\}$$

is a basis for $L(D)$.

(b) If D is not effective but $deg(D) \ge 0$ then write $D = dP + D'$, where $deg(D') = 0$, $d > 0$, and P is any point. Let $q(x) \in L(D')$ (which is a 1-dimensional vector space) be any non-zero element. Then

$$\{m_P(x)^i q(x) \mid 0 \le i \le d\}$$

is a basis for $L(D)$.

(c) If $deg(D) < 0$ then $L(D) = \{0\}$.

Now that we know how to compute bases for Riemann-Roch spaces, it is relatively easy to make fairly explicit the G-module structure of $L(D)$.

Theorem 6. *Let X, $G \subset \mathrm{Aut}(X) = PGL(2, F)$, and $D = \sum_{i=0}^{s} a_i P_i$ be a G-equivariant divisor as above. Assume F is algebraically closed. Let $\rho : G \to \mathrm{Aut}(L(D))$ denote the associated representation. This acts trivially on the constants (if any) in $L(D)$; we denote this action by 1. Let $S = \mathrm{supp}(D)$ and let*

$$S = S_1 \cup S_2 \cup ... \cup S_m$$

be the decomposition of S into primitive G-sets (orbits).

(a) If D is effective then

$$\rho \cong 1 \oplus_{i=1}^{m} \rho_i,$$

where ρ_i is a representation on the subspace

$$V_i = \langle m_{P_j}(x)^{\ell_j} \mid 1 \leq \ell_j \leq a_j,\ P_j \in S_i \rangle,$$

satisfying $dim(V_i) = \sum_{P_j \in S_i} a_j$, for $1 \leq i \leq m$. Here $\langle ... \rangle$ denotes the vector space span.

(b) If $deg(D) > 0$ but D is not effective then ρ is a subrepresentation of $\rho : G \to Aut_F\, L(D')$, where D' is a G-equivariant effective divisor satisfying $D' \geq D$.

Note that (b) allows one to reduce to case (a). For further details, see [JT].

In fact, each of these subrepresentations ρ_i is induced from a one-dimensional character of the group G_{P_i} (i.e., ρ_i is "monomial"). Here's why. The above theorem implies that

$$[V_i] = [L(\sum_{1 \leq j \leq s} D_j)] - [L(\sum_{j \neq i} D_j)].$$

where D_j is the divisor associated to the orbit S_j, $D = \sum_{j=1}^{s} D_j$ and $\mathrm{supp}(D_j) = S_j$. Borne's Lemma 10 implies

$$[L(\sum_{1 \leq j \leq s} D_j)] - [L(\sum_{j \neq i} D_j)] = \deg_{eq}(D_i).$$

(In this case the ramification module is trivial but that doesn't even matter since it cancels in the above difference.) The definition of the equivariant degree implies that ρ_i is monomial.

3 Algorithms in the hyperelliptic curve case

Let X be a smooth projective hyperelliptic curve defined over F. In this case, MAGMA can compute the automorphism group G of X. In fact, Florian Hess has recently (May, 2005) extended this MAGMA command for computing automorphism groups to much more general (planar) curves, so now the computations described here can be extended. For examples (using GAP) involving the modular curves (which are in general not planar), see [JK2].

The code for the algorithms discussed here is given in an appendix.

3.1 Computing G-equivariant divisors

We have written a MAGMA program `G-equivariant-orbit` which computes the orbit of a point in a hyperelliptic curve C defined over a finite field under the action of the group G and uses it to construct an associated G-equivariant divisor D on C. The input is a hyperelliptic curve C defined over a finite field, and a point P on the curve. The program outputs the effective divisor $D = \sum_{Q \in G \cdot P} Q$ on the curve whose support is the G-orbit of P, where G is the automorphism group of C over F. It does so by computing the automorphism group (MAGMA has a command to do this), regarded as a group acting on the set of rational points of C. In fact, Florian Hess has recently (May, 2005) extended this MAGMA command for computing automorphism groups to much more general curves, so now our program `G-equivariant-orbit` works more generally as well.

We describe this in terms of an example:

```
F:=CyclotomicField(4);
f:=x^5-x;
P<x>:=PolynomialRing(F);
C:=HyperellipticCurve(f);
g:=Genus(C);
G, m, A := AutomorphismGroup(C); //A4
G_list:=[g : g in G];
P:=Points(C,0);
Div:=DivisorGroup(C);
orbit:={};
for j0 in [1..12] do
 g0:=G_list[j0];
 orbit:=orbit join {m(g0)(P[1])};
end for;
I:=SetToIndexedSet(orbit);
D0:=&+[Divisor(I[i]) : i in [1..#I]];
```

3.2 The decomposition of the Riemann-Roch space

This section describes an algorithm, which has been implemented in MAGMA (see Appendix), which computes the matrix representation of the Riemann-Roch space of a G-equivariant divisor D at a group element with respect to the basis of $L(D)$ provided by MAGMA. The input is a hyperelliptic curve C defined over a field[2], a G-equivariant divisor D, and an element g of the automorphism group of C. The program computes the divisor D from P using the algorithm described in the previous section and then outputs the matrix $\rho(g)$ with respect to the basis of $L(D)$ provided by MAGMA. The idea is as follows. Let $\mathcal{B} = \{b_1, ..., b_k\}$ denote (rational) functions forming the basis of $L(D)$. First, the program makes explicit how the group acts on $\mathcal{B}$. Next, note each row of $\rho(g)$ represents a relationship of the form

$$\rho(g)b_j = a_{1,j}b_1 + a_{2,j}b_2 + ... + a_{k,j}b_k,$$

for some matrix coefficients $a_{i,j}$ depending on g. The problem is to solve for these coefficients. In some cases, GAP can simply solve for these coefficients using the command `Coefficients`, after defining the vector space $V = Span(b_1, ..., b_k)$.

More generally, there is the following trick: These coefficients themselves may be regarded as solutions to a linear system

$$\rho(g)b_j(P_\ell) = a_{1,j}b_1(P_\ell) + a_{2,j}b_2(P_\ell) + ... + a_{k,j}b_k(P_\ell), \qquad \ell = 1, 2, ..., k,$$

where the P_ℓ are points on the curve where the functions are well-defined. In fact, they need not be on the curve C, but merely any points in the ambient space where all the functions are defined (possibly after enlarging the field of definition). These linear systems can be solved, thus computing the desired matrix $\rho(g) = (a_{ij})$. Once this is known for each g, the decomposition of $L(D)$ can be determined from character tables of G. (Since MAGMA does not have Brauer tables, at least not of version 2.10, this is easier said than done when the characteristic of F divides the order of G. However, they can be sent over to GAP which does have modular character commands.)

See §4.4 for illustrations.)

[2]When the field is finite and "too small" the program implementing this algorithm algorithm can fail. In this case, it enters an infinite loop and MAGMA eventually crashes from lack of memory.

4 The general curve case

Let X be a smooth projective curve defined over F.

4.1 Bounds on the size of the irreducible submodules of $L(D)$

Suppose $G \subset \mathrm{Aut}_F(X)$ is a finite subgroup, either $\mathrm{char}(F) = 0$ or $p = \mathrm{char}(F)$ does not divide $|G|$, and that the divisor $D \neq 0$ on X is stable by G. Let d_0 denote the smallest size of a G-orbit on X. (For example, if $X(k)$ has G-fixed point then $d_0 = 1$.)

Theorem 7. *The natural representation of G on $L(D)$ decomposes as a direct sum of irreducible subrepresentations of dimension $\leq d_0$.*

Remark 1. *This is best possible in the sense that irreducible subspaces of dimension d_0 can occur in some situations, by Theorem 6 above.*

The assumption that p does not divide $|G|$ can be dropped but one must replace "The natural representation of G on $L(D)$ decomposes as a direct sum of irreducible subrepresentations of dimension $\leq d_0$" by "Each irreducible composition factor of the representation of G on $L(D)$ has dimension $\leq d_0$".

The introduction said there would be no proofs, which was a lie. This one is too short and sweet to be left out.

proof: Let $E \neq 0$ be an effective G-invariant divisor of minimal degree d_0. Let $d = [\deg(D)/d_0]$ denote the integer part. The group G acts on each space in the series

$$\begin{gathered}\{0\} = L(-(d+1)E + D) \subset L(-dE + D) \\ \subset L(-(d-1)E + D) \subset \\ .. \subset L(-(d-m)E + D) \subset ... \subset L(D)\ .\end{gathered}$$

In particular, G acts on the successive quotient spaces

$$L(-(d-m-1)E + D)/L(-(d-m)E + D), \qquad 0 \leq m \leq d-1,$$

by "the" quotient representation. These are all of dimension at most d_0.

If F has characteristic 0 then every finite dimensional representation of a finite group is semi-simple. If F has characteristic p and p does not divide $|G|$ then every finite dimensional representation of G is semi-simple (Mascke's Theorem). From these, the theorem follows. $\square$

Corollary 8. *Suppose that $G \subset Aut_F(X)$ is a finite non-abelian group acting on a smooth projective curve X defined over an algebraically closed field F and assume $\pi : X \to X/G$ is unramified. Let d_0 be as in Theorem 7 and let d_G denote the largest degree of all irreducible (F-modular) representations of G. Then*

$$d_0 \geq d_G.$$

Using Theorem reftheorem:2, the assumption "$\pi : X \to X/G$ is unramified" can be replaced by "either $\mathrm{char}(F) = 0$ or $p = \mathrm{char}(F)$ does not divide $|G|$."

4.2 Borne's formula

For any point $P \in X(k)$, let G_P be the decomposition group at P (i.e. the subgroup of G fixing P). Since char k is zero, the quotient $\pi : X \to Y = X/G$ is tamely ramified[3] and this group G_P is cyclic. G_P acts on the cotangent space of $X(k)$ at P by a k-character. This character is the **ramification character** of X at P.

The **ramification module** is defined by

$$\Gamma_G = \sum_{P \in X(k)_{ram}} Ind_{G_P}^G \left(\sum_{\ell=1}^{e_P - 1} \ell \psi_P^\ell \right),$$

where e_P is the size of the inertia group, and ψ_P is the ramification character at P. By a result of Nakajima, there is a unique G-module $\tilde{\Gamma}_G$ such that

$$\Gamma_G = |G| \tilde{\Gamma}_G.$$

We abuse terminology and also call $\tilde{\Gamma}_G$ the **ramification module**.

Now consider a G-equivariant divisor D on $X(k)$. If $D = \frac{1}{e_P} \sum_{g \in G} g(P)$ then we call D a **reduced orbit**. The reduced orbits generate the group of G-equivariant divisors $Div(X)^G$.

Definition 9. *The **equivariant degree** is a map from $Div(X)^G$ to the Grothendieck group $R_k(G) = \mathbb{Z}[G_k^*]$ of virtual k-characters of G,*

$$deg_{eq} : Div(X)^G \to R(G),$$

defined by the following conditions:

[3] However, this is not needed for Borne's formula.

1. *deg_{eq} is additive on G-equivariant divisors of disjoint support,*

2. *If $D = r\frac{1}{e_P}\sum_{g\in G} g(P)$ is an orbit then*

$$deg_{eq}(D) = \begin{cases} Ind_{G_P}^G(\sum_{\ell=1}^{r}\psi^{-\ell}), & \text{if } r > 0, \\ -Ind_{G_P}^G(\sum_{\ell=0}^{-(r+1)}\psi^{\ell}), & \text{if } r < 0, \\ 0, & r = 0, \end{cases}$$

where $\psi = \psi_P$ is the ramification character of X at P.

Note: In general, this is not additive (except on those divisors which are pull-backs via π).

If $D = \pi^*(D_0)$ is the pull-back of a divisor $D_0 \in Div(Y)$ then $deg_{eq}(D)$ has a very simple form. In this case, r is a multiple of e_P, so the equivariant degree on each orbit is r/e_P times $Ind_{G_P}^G$ of the regular representation of G_P. In this case, we have

$$deg_{eq}(D) = deg(D_0)[k[G]], \tag{1}$$

We recall the following formula of Neils Borne [Bo].

Lemma 10. *(**Borne's formula**) If D is a G-equivariant nonspecial divisor, then the (virtual) character of $L(D)$ is given by*

$$[L(D)] = (1 - g_Y)[k[G]] + [deg_{eq}(D)] - [\tilde{\Gamma}_G], \tag{2}$$

where Y is the quotient of X by G, g_Y is its genus, $\deg_{eq}(D)$ is the equivariant degree of D, and $\tilde{\Gamma}_G$ is the ramification module.

Köch gives more explicit expressions for $L(D)$, even under more general conditions then we have assumed here, but they are rather technical [K]. Note that in the case where $D = \pi^*(D_0)$, Borne's formula tells us that

$$[L(D)] = (1 - g_Y + deg(D_0))[k[G]] - [\tilde{\Gamma}_G].$$

4.2.1 Computing the ramification module

Let ρ_1, ..., ρ_k denote a complete set of irreducible $\mathbb{Q}[G]$-modules.

A special case of the main theorem in [JK] is the following result.

Theorem 11. *If $\tilde{\Gamma}_G$ and $L(D)$ have a $\mathbb{Q}[G]$-module structure, then*

$$\tilde{\Gamma}_G \simeq \bigoplus_j (m_j^2 d_j)^{-1} (\sum_\ell (\dim(\rho_j) - \dim(\rho_j^{H_\ell})) \frac{R_\ell}{2}) \rho_j.$$

Here the first sum is over the set $G^*_{\mathbb{Q}}$ of all irreducible $\mathbb{Q}[G]$-modules, the second sum is over all conjugacy classes of cyclic subgroups of G, H_ℓ is a representative cyclic subgroup, $\rho_j^{H_\ell}$ indicates the dimension of the fixed part of ρ_j under the action of H_ℓ, R_ℓ denotes the number of branch points in Y where the decomposition group is conjugate to H_ℓ, m_j denotes the Schur index of ρ_j (the degree of the field generated by the character values $\chi_j(g)$ in the field generated by the matrix coefficients of $\rho_j(g)$), and d_j denotes the number of distinct irreducible $\mathbb{C}[G]$-modules in $\rho_j \otimes \mathbb{C}$.

Our result is more general than this but the statement is more technical to state (see [JK] for details). However, Example 14 illustrates the more general result. See also [JK2] for another detailed example.

4.2.2 A formula for the multiplicity

Let $F = \mathbb{C}$ in this subsection.

For each conjugacy class $\gamma_i \in G_*$, pick a cyclic subgroup H_i generated by a $g \in \gamma_i$.

Let ρ denote an irreducible representation of G, let H be a cyclic subgroup, and denote by $n_{\rho,j} = n_{\rho,j}(H) \geq 0$ the integers defined by

$$Res_H(\rho) = \sum_{j=1}^{|H|} n_{\rho,j} \psi^j, \tag{3}$$

where ψ is a primitive character of H. Note that $n_{\rho,j} = n_{\rho,j+|H|}$ and

$$\sum_{j=1}^{|H|} n_{\rho,j} = \dim(\rho). \tag{4}$$

Recall that $Div(X)^G$ is generated by orbits $r \sum_{g \in G/G_P} g(P)$. If $\mathrm{supp}(D) = \cup_{i=1}^s \{g(P_i) \mid g \in G/G_{P_i}\}$, is a disjoint union then we write $\mathrm{supp}(D)/G = \{P_i \mid 1 \leq i \leq s\}$. In this case, we may write D uniquely as

$$D = \sum_{P \in \mathrm{supp}(D)/G} r_P \sum_{g \in G/G_P} g(P),$$

for some $r_P \in \mathbb{Z}$.

Let $L(D)_\rho$ denote the ρ-isotypical component of $L(D)$

Another consequence of Borne's formula is the following formula.

Theorem 12. *Let $F = \mathbb{C}$, $G \subset Aut(X)$, and let D be a G-equivariant nonspecial divisor. Assume all the irreducible characters of G are rational-valued. The multiplicity of an irreducible representation ρ of G in $L(D)$ is given by*

$$\dim(L(D)_\rho) = \dim(\rho)(1-g(X_G)) + \sum_{P \in \mathrm{supp}(D)/G} T_{P,\rho} - \sum_{\ell} (\dim(\rho) - \dim(\rho^{H_\ell}))\frac{R_\ell}{2}, \tag{5}$$

where

$$T_{P,\rho} = \begin{cases} \sum_{\ell=1}^{r_P} n_{\rho,\ell}(G_P) = \sum_{\ell=1}^{r_P} \langle \psi_P^\ell, \mathrm{Res}_{H_\ell}^G \rho \rangle, & r_P > 0, \\ -\sum_{\ell=0}^{-(r_P+1)} n_{\rho,-\ell}(G_P) = \sum_{\ell=1}^{-(r_P+1)} \langle \psi_P^{-\ell}, \mathrm{Res}_{H_\ell}^G \rho \rangle, & r_P < 0, \end{cases}$$

ρ^{H_ℓ} denotes the restriction of ρ to H_ℓ, $R_\ell = R(H_\ell)$ is the number of branch points with decomposition group conjugate to H_ℓ, and ρ_1, ..., ρ_k are as in Theorem 11.

The next section gives an example.

4.3 Examples: good characteristic

Example 13. *Consider the genus 2 curve*

$$y^2 = x(x-2)(x-4), \qquad z^2 = x+4,$$

over $F = \mathbb{C}$. This has an action of $G = C_2 \times C_2$ given by

$$\begin{aligned} \alpha &: (x,y,z) \longmapsto (x,-y,z), \\ \beta &: (x,y,z) \longmapsto (x,y,-z), \\ \alpha\beta &: (x,y,z) \longmapsto (x,-y,-z). \end{aligned}$$

This group has character table

	1	α	β	$\alpha\beta$
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1

The divisor

$$D = (0,0,2) + (0,0,-2) + (-4, 8\sqrt{3}, 0) + (-4, -8\sqrt{3}, 0)$$

is G-equivariant and supp$(D)/G = \{(0,0,2), (-4, 8\sqrt{3}, 0)\}$. One can show

$$L(D) = \{a_0 + a_1 \frac{1}{t} + a_2 \frac{y}{xt}\}.$$

Direct computation: This Riemann-Roch space splits up into a direct sum of irreducible 1-dimensional G-modules. As a matrix representation,

$$\rho(\alpha^i \beta^j) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & (-1)^j & 0 \\ 0 & 0 & (-1)^{i+j} \end{pmatrix}.$$

The character of ρ agrees with $\chi_1 + \chi_2 + \chi_4$ on G, so

$$L(D) \cong \rho_1 \oplus \rho_2 \oplus \rho_4.$$

Geometric computation using the formula: We have

$$\dim(\rho)(1 - g(X_G)) = 1,$$

for each irreducible ρ.

Note that each orbit of G in supp(D) is represented by a point P where the decomposition group is $G_P = C_2$ and the multiplicity of the orbit is $r_P = 1$. Therefore,

$$T_{P,\rho} = \begin{cases} 0, & \rho = \rho_i, \ i = 1, \\ 1, & \rho = \rho_i, \ i = 2, 3, \\ 2, & \rho = \rho_4. \end{cases}$$

For $\rho = 1$, we therefore have

$$\dim(L(D)_\rho) = 1 + 0 - 0 = 1.$$

This means that $L(D)$ contains the trivial representation ρ_1 with multiplicity 1, as predicted.

The cover $X \to X/G$ has 5 branch points: three with inertia group $G_P = C_2 = \{1, \alpha\}$ (at $x = 0, 2, 4$), one with inertia group $G_P = C_2 = \{1, \beta\}$ (at

$x = -4$), and one with inertia group $G_P = C_2 = \{1, \alpha\beta\}$ (at $x = \infty$). This means

$$R(\{1, \alpha\}) = 3, \quad R(\{1, \beta\}) = 1, \quad R(\{1, \alpha\beta\}) = 1.$$

Plugging these into the formula in Theorem 12 yields $\chi_1 + \chi_2 + \chi_4$ for the character of $L(D)$.

Example 14. *We consider the example of the genus 3 Klein quartic over various ground fields.*

If k contains the cyclotomic field $\mathbb{Q}(\zeta_7)$ of seventh roots of unity and if C is the curve $X^3Y + Y^3Z + Z^3X = 0$ then the cyclic group of order 3 acts on X by cyclically permuting the coordinates and the cyclic group of order 7 acts by sending $(X : Y : Z) \longmapsto (\zeta_7 X : \zeta_7^4 Y : \zeta_7^2 Z)$.

Let $G \cong C_3 \rtimes C_7$ be the semi-direct product of these groups. This has character table[4]:

	$1a$	$3a$	$7a$	$3b$	$7b$
ρ_1	1	1	1	1	1
ρ_2	1	ζ_3^2	1	ζ_3	1
ρ_3	1	ζ_3	1	ζ_3^2	1
ρ_4	3	0	$\zeta_7^3 + \zeta_7^5 + \zeta_7^6$	0	$\zeta_7 + \zeta_7^2 + \zeta_7^4$
ρ_5	3	0	$\zeta_7 + \zeta_7^2 + \zeta_7^4$	0	$\zeta_7^3 + \zeta_7^5 + \zeta_7^6$

The conjugacy classes for the columns are as given by GAP's `ConjugacyClasses` *command (the same ordering is used by MAGMA in this case).*

The points of degree 1 on X/k include $P_1 = (1 : 0 : 0)$, $P_2 = (0 : 1 : 0)$, and $P_3 = (0 : 0 : 1)$. The divisor $P_1 + P_2 + P_3$, and all its multiples, is G-equivariant. The functions

$$1, \quad X/Z, \quad Y/X, \quad Z/Y,$$

form a basis of $L(D)$, where $D = 2(P_1 + P_2 + P_3)$. The functions

$$1, \quad X/Z, \quad Y/X, \quad Z/Y, \quad X/Y, \quad Z/X, \quad Y/Z,$$

form a basis of $L(D)$, where $D = 3(P_1 + P_2 + P_3)$. The first space is, as a G-module, not defined over $\mathbb{Q}$. In fact, it is the direct sum of the trivial

[4]This was obtained using [Gap]. Incidently, there is only one non-cyclic group of order 21, up to isomorphism.

representation ρ_1 and the 3-dimensional representation ρ_4. The second space is rational as a G-module. In fact, it is the direct sum of ρ_1, ρ_4 and ρ_5. These facts may be verified by computing the trace directly using the above basis.

If k does not contain ζ_7 then only C_3 acts on the curve X/k. The space $L(D)$, where $D = 2(P_1 + P_2 + P_3)$, decomposes into the C_3-modules

$$\langle 1\rangle \oplus \langle x/z, y/x, z/y\rangle = \langle 1\rangle \oplus \langle x/z + y/x + z/y\rangle \oplus V,$$

where V is a 2-dimensional C_3-module. If k contains the cyclotomic field $\mathbb{Q}(\zeta_3)$ then V decomposes into a direct sum of two irreducible 1-dimensional C_3-modules. If k does not contain the cyclotomic field $\mathbb{Q}(\zeta_3)$ then V is irreducible as a C_3-module.

Points of ramification are determined as follows:

- *C_3 action: The points ramified from the cyclic action on the coordinates X, Y, Z of $\mathbb{P}^2$ are: $(1:1:1)$, $(1:\zeta_3:\zeta_3^2)$, and $(1:\zeta_3^2:\zeta_3)$. Of these, only $P_4 = (1:\zeta_3:\zeta_3^2)$ and $P_5 = (1:\zeta_3^2:\zeta_3)$. are in $X(k)$ (assuming k contains ζ_3). We have*

$$G_{P_4} \cong C_3, \qquad G_{P_5} \cong C_3.$$

- *C_7 action: The points ramified from the above action of C_7 on the coordinates X, Y, Z of $\mathbb{P}^2$ are: P_1, P_2, and P_3, all of which belong to $C(k)$. We have $G_{P_i} \cong C_7$, for $i = 1, 2, 3$.*

There is one orbit of points where the inertia group is isomorphic to C_7. There are two orbits of points where the inertia group is isomorphic to C_3. This allows us to compute the number of branch points in X/G where the inertia group is conjugate to H_ℓ:

$$\deg R_\ell = \begin{cases} 2, & \text{if } H_\ell = C_3, \\ 1, & \text{if } H_\ell = C_7, \\ 0, & \text{otherwise.} \end{cases}$$

How does C_7 act on the co-tangent space $T_{P_1}(X)^*$ at P_1? Local coordinates on the patch containing P_1 are $y = Y/X$, $z = Z/X$, and the equation for C on the patch is $y + y^3z + z^3 = 0$. Since $(3y^2z + 1)dy + (y^3 + 3z^2)dz = 0$, the co-tangent space has basis $dz/(3y^2z + 1) = -dy/(y^3 + 3z^2)$. The map $\tau : (X : Y : Z) \longmapsto (X : \zeta_7^3 Y : \zeta_7 Z)$ maps $\frac{dy}{y^3+3z^2} \longmapsto \zeta_7 \frac{dy}{y^3+3z^2}$.

How does C_7 act on the co-tangent space $T_{P_2}(X)^*$ at P_2? Local coordinates on the patch containing P_2 are $x = X/Y$, $z = Z/Y$, and the equation for C on the patch is $x^3 + z + z^3x = 0$. Since $(3x^2 + z^3)dx + (1 + 3z^2x)dz = 0$, the co-tangent space has basis $dx/(3z^2x + 1)$. The map $\tau : (X : Y : Z) \longmapsto (X : \zeta_7^3 Y : \zeta_7 Z)$ maps $\frac{dx}{3z^2x+1} \longmapsto \zeta_7^4 \frac{dx}{3z^2x+1}$.

How does C_7 act on the co-tangent space $T_{P_3}(X)^*$ at P_3? Local coordinates on the patch containing P_3 are $x = X/Z$, $y = Y/Z$, and the equation for C on the patch is $x^3y + x + y^3 = 0$. Since $(3y^2 + x^3)dy + (1 + 3x^2y)dx = 0$, the co-tangent space has basis $dy/(3x^2y + 1)$. The map $\tau : (X : Y : Z) \longmapsto (X : \zeta_7^3 Y : \zeta_7 Z)$ maps $\frac{dy}{3x^2y+1} \longmapsto \zeta_7^2 \frac{dy}{3x^2y+1}$.

How does C_3 act on the co-tangent space $T_{P_4}(X)^*$ at P_4? The patch $Z = 1$ with local coordinates $x = X/Z$ and $y = Y/Z$ contains $P_4 = (\zeta_3 : \zeta_3^2 : 1)$. Again, the co-tangent space has basis $dy/(3x^2y + 1) = -dx/(x^3 + 3y^2)$. The action of the group C_3 is generated by by $(X : Y : Z) \longmapsto (Y : Z : X)$. In terms of the local coordinates, this sends

$$x \longmapsto y/x, \quad y \longmapsto 1/x.$$

Note $d(y/x) = -\frac{y}{x^2}dx + \frac{1}{x}dy = -dx + \zeta_3^2 dy$ and $d(1/x) = -\frac{1}{x^2}dx = -\zeta_3 dx$ at P_4. Therefore, this C_3 action is generated by the map which sends

$$dx \longmapsto d(y/x) = dx + \zeta_3^2 dy, \quad dy \longmapsto d(1/x) = -\zeta_3 dx,$$

and hence

$$\frac{dy}{3x^2y + 1} \longmapsto \frac{-\zeta_3 dx}{3(y/x)^2(1/x) + 1} = \zeta_3 \frac{dy}{3x^2y + 1}.$$

The ramification module is determined as follows. By definition,

$$\Gamma_G = \sum_{\mathcal{O}} \sum_{P \in \mathcal{O}} Ind_{G_P}^G \Big(\sum_{\ell=1}^{e_P - 1} \ell \psi_P^\ell \Big),$$

where the outer sum over runs over all G-orbits[5] $\mathcal{O}$, e_P denotes the inertia degree[6], and ψ_P denotes the character of G_P acting on the co-tangent space. Let us identify ζ_7 with the identity character on $G_P = C_7$ and similarly for ζ_3 on $G_P = C_3$. On the G-orbit of $P = (1 : 0 : 0)$, we have

[5]Namely, the G-orbit of $(1 : 0 : 0)$ with inertia group C_7, the G-orbit of $(1 : \zeta_3 : \zeta_3^2)$ with inertia group C_3, and the G-orbit of $(1 : \zeta_3^2 : \zeta_3)$ with inertia group C_3.

[6]That is, the size of the inertia group of P.

$$\begin{gathered}\sum_{P\in\mathcal{O}} Ind_{G_P}^G(\sum_{\ell=1}^{e_P-1}\ell\psi_P^\ell)\\ = Ind_{C_7}^G(\zeta_7+2\zeta_7^2+...+6\zeta_7^6)+\\ Ind_{C_7}^G(\zeta_7^2+2\zeta_7^4+...+6\zeta_7^{12})+\\ Ind_{C_7}^G(\zeta_7^4+2\zeta_7^4+...+6\zeta_7^{24})\\ = (1+2+4)Ind_{C_7}^G(\zeta_7+\zeta_7^2+\zeta_7^4)\\ +(3+5+6)Ind_{C_7}^G(\zeta_7^3+\zeta_7^5+\zeta_7^6).\end{gathered}$$

On the G-orbit of $P=(1:\zeta_3:\zeta_3^2)$, we have

$$\sum_{P\in\mathcal{O}} Ind_{G_P}^G(\sum_{\ell=1}^{e_P-1}\ell\psi_P^\ell) = Ind_{C_3}^G(7(\zeta_3+2\zeta_3^2)),$$

and on the G-orbit of $P=(1:\zeta_3:\zeta_3^2)$, we have

$$\sum_{P\in\mathcal{O}} Ind_{G_P}^G(\sum_{\ell=1}^{e_P-1}\ell\psi_P^\ell) = Ind_{C_3}^G(7(\zeta_3^2+2\zeta_3)).$$

Putting these together, we have

$$\Gamma_G = 7Ind_{C_7}^G(\zeta_7+\zeta_7^2+\zeta_7^4)+14Ind_{C_7}^G(\zeta_7^3+\zeta_7^5+\zeta_7^6)+21Ind_{C_3}^G(\zeta_3+\zeta_3^2).$$

The character table of G can be used to determine the decomposition of this representation into irreducibles. We have

$$\Gamma_G = 21\chi_2+21\chi_3+63\chi_4+84\chi_5,$$

where $\chi_i=\operatorname{tr}\rho_i$ $(i=1,2,...,5)$ denote the irreducible characters in the table above. This gives

$$\tilde{\Gamma}_G = \frac{1}{|G|}\Gamma_G = \chi_2+\chi_3+3\chi_4+4\chi_5.$$

Under the action of the Galois group C generated by σ and τ, where $\sigma:\zeta_3\mapsto\zeta_3^{-1}$ and $\tau:\zeta_7\mapsto\zeta_7^{-1}$, we have $\tau(\tilde{\Gamma}_G)=\chi_2+\chi_3+4\chi_4+3\chi_5$ and $\sigma(\tilde{\Gamma}_G)=\tilde{\Gamma}_G$.

Next, we compute the equivariant degree of the G-equivariant divisors $D_r=r(P_1+P_2+P_3)$, for $r=2,3$. Recall that $P_1+P_2+P_3$ is the G-orbit of P_3. Using the ramification character ζ_7 of $G_{P_3}\cong C_7$, we have

$$deg_{eq}(D_2) = Ind_{C_7}^G(\zeta_7^{-1} + \zeta_7^{-2}) = Ind_{C_7}^G(\zeta_7^5 + \zeta_7^6),$$

and

$$deg_{eq}(D_3) = Ind_{C_7}^G(\zeta_7^{-1} + \zeta_7^{-2} + \zeta_7^{-3}) = Ind_{C_7}^G(\zeta_7^4 + \zeta_7^5 + \zeta_7^6).$$

Using the character table of G, we find

$$deg_{eq}(D_2) = 2\chi_5, \qquad deg_{eq}(D_3) = \chi_4 + 2\chi_5.$$

This is enough data to use Borne's formula to compute the class of the Riemann-Roch space of D_r, $r = 1, 2$. We have,

$$\begin{gathered}[L(D_2)] = k[G] + deg_{eq}(D_2) - \tilde{\Gamma}_G \\ = (\chi_1 + \chi_2 + \chi_3 + 3\chi_4 + 3\chi_5) \\ +2\chi_5 - (\chi_1 + \chi_2 + \chi_3 + 3\chi_4 + 4\chi_5) \\ = \chi_1 + \chi_5,\end{gathered}$$

and

$$\begin{gathered}[L(D_3)] = k[G] + deg_{eq}(D_2) - \tilde{\Gamma}_G \\ = (\chi_1 + \chi_2 + \chi_3 + 3\chi_4 + 3\chi_5) \\ +(\chi_4 + 2\chi_5) - (\chi_1 + \chi_2 + \chi_3 + 3\chi_4 + 4\chi_5) \\ = \chi_1 + \chi_4 + \chi_5.\end{gathered}$$

This is enough data to use our formula to compute the Galois orbit of the class of the ramification module for G. We have

$$dim(\chi_1 + \chi_2)^{C_3} = 0, \qquad dim(\chi_1 + \chi_2)^{C_7} = 2,$$

$$dim(\chi_4 + \chi_5)^{C_3} = 2, \qquad dim(\chi_4 + \chi_5)^{C_7} = 0.$$

We have already computed $R_{C_3} = 2$, $R_{C_7} = 2$, so the formula of our theorem computes $\tilde{\Gamma}_G + \tau\tilde{\Gamma}_G$ to be

$$2\chi_1 + 2\chi_2 + 7\chi_4 + 7\chi_5,$$

which agrees with our calculation above.

Example 15. *Let $F = \mathbb{Q}(i)$ and let C denote the curve defined by*

$$y^2 = x^5 - x.$$

This has genus 2. The automorphism group $G = Aut_F(C) \cong SL(2,3)$ is a central 2-fold cover of A_4: we have a short exact sequence,

$$1 \to Z \to G \to A_4 \to 1,$$

where Z denotes the center (containing the hyperelliptic involution of C). Over $\mathbb{C}$, the character table of G:

Class	*1*	*2*	*3*	*4*	*5*	*6*	*7*
Size	*1*	*1*	*4*	*4*	*6*	*4*	*4*
Order	*1*	*2*	*3*	*3*	*4*	*6*	*6*
χ_1	*1*	*1*	*1*	*1*	*1*	*1*	*1*
χ_2	*1*	*1*	ω	*-1-*ω	*1*	ω	*-1-*ω
χ_3	*1*	*1*	*-1-*ω	ω	*1*	*-1-*ω	ω
χ_4	*2*	*-2*	*-1*	*-1*	*0*	*1*	*1*
χ_5	*2*	*-2*	*1+*ω	*-*ω	*0*	*-1-*ω	ω
χ_6	*2*	*-2*	*-*ω	*1+*ω	*0*	ω	*-1-*ω
χ_7	*3*	*3*	*0*	*0*	*-1*	*0*	*0*

where ω denotes a cube root of unity.

Let O be the orbit of the group G acting on the point at infinity[7] *in $C(F)$ and let D be the simple effective divisor whose support is O. Then $L(D)$ is 5-dimensional. Let $\rho : G \to Aut_F(L(mD))$ denote the natural action of G on $L(mD)$. Using MAGMA, we can compute this matrix representation with respect to the basis of $L(D)$ given by MAGMA. If $G_* = \{\gamma_1 = \{1\}, \gamma_2, ..., \gamma_7\}$ are the conjugacy classes of G then there are representatives $g_i \in \gamma_i$, $1 \leq i \leq 12$, such that*

m	$(\operatorname{tr}\rho(g_1), ..., \operatorname{tr}\rho(g_7))$
1	*(5,-3,2,2,1,0,0)*
2	*(11,3,2,2,-1,0,0)*
3	*(17,-3,2,2,-1,0,0)*
4	*(23,3,2,2,-1,0,0)*
5	*(29,-3,2,2,-1,0,0).*

[7]MAGMA views the curve as embedded in a weighted projective space, with weights 1, 3, and 1, in which the point at infinity is nonsingular.

We conjecture, based on this, that the character of $L(mD)$ is

$$(5+6(m-1),(-1)^{m-1}3,2,2,-1,0,0), \qquad m \geq 2. \tag{6}$$

In any case, this table and the character table for G imply that ρ decomposes as follows:

m	*decomposition of trace* ρ
1	$\chi_1+\chi_2+\chi_3$
2	$\chi_1+\chi_5+\chi_6+2\chi_7$
3	$\chi_1+\chi_4+2\chi_5+2\chi_6+2\chi_7$
4	$\chi_1+3\chi_4+4\chi_5+4\chi_6+2\chi_7$
5	$\chi_1+4\chi_4+5\chi_5+5\chi_6+2\chi_7$

Indeed, if $\operatorname{tr}\rho-\chi_1$ has character values $(\alpha_1,...,\alpha_7)$ then one can explicitly compute the multiplicities in terms of these α_i's:

- *the multiplicity of $\chi_2+\chi_3$ in ρ is $-\frac{\alpha_3+\alpha_7}{7}$,*
- *the multiplicity of χ_4 in ρ is $-\frac{\alpha_1-4\alpha_3-3\alpha_5}{6}$,*
- *the multiplicity of $\chi_5+\chi_6$ in ρ is $-\frac{\alpha_1-\alpha_3-3\alpha_5-3\alpha_7}{6}$,*
- *the multiplicity of χ_7 in ρ is $-\alpha_3-\alpha_5-\alpha_7$.*

Assuming the conjecture (6) is correct, then the character of $L(mD)$ would be

$$\operatorname{trace}\rho=\chi_1+m\chi_4+(m+1)\chi_5+(m+1)\chi_6+2\chi_7, \qquad m\geq 2.$$

4.4 Examples: bad characteristic

4.4.1 General remarks

In general, if C is a curve defined over a field F with finite automorphism group $G=Aut_F(C)$ then we call G **large** if $|G|>|C(F)|$.

Lemma 16. *If G is large then every point of $C(F)$ is ramified for the covering $C\to C/G$.*

proof: Suppose $P \in C(F)$ is not ramified, so the stabilizer of P, G_P, is trivial. In this case, $|G \cdot P| = |G|/|G_P| = |G|$. But $G \cdot P \subset C(F)$ so $|G \cdot P| \leq |C(F)|$, a constradiction. $\square$

Let $p \geq 3$ be a prime and let C denote the curve defined by

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

This has genus $\frac{p-1}{2}$.

Example 17. *Let $F = GF(p)$.*

We assume that the automorphism group $G = Aut_F(C)$ is a central 2-fold cover of $PSL(2,p)$, we have a short exact sequence,

$$1 \to Z \to G \to PSL_2(p) \to 1, \tag{7}$$

where Z denotes the subgroup of G generated by the hyperelliptic involution (which coincides with the center of G). The group G has order $2|PSL(2,p)| = p(p^2-1)$. The following transformations generate G:

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

where $a \in F^\times$ is a primitive $(p-1)$-st root of unity.

Let $P_1 = (1:0:1)$ and let H be its stabilizer in G. A counting argument shows that H is a solvable group of order $2p(p-1)$ generated by γ_1, $\gamma_2(a)$ and γ_3. By Lemma 16, every point in

$$C(F) = \{(1:0:0), (0:0:1), (1:0:1), ..., (p-1:0:1)\}$$

is ramified over the covering $C \to C/G$ in the sense that each stabilizer $G_P = Stab_G(P)$ is non-trivial, $P \in C(F)$. The group G acts transitively on $C(F)$.

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

$$x^i y^j, \qquad 0 \leq i \leq p-1,\ j \geq 0,\ 2i + pj \leq m.$$

Lemma 18. *The semisimplification ρ_{ss} of the representation ρ of H acting on $L(D)$ is the direct sum of one-dimensional representations of G.*

proof: *The generator γ_1 acts trivially on the basis of $L(D)$, whereas*

$$\gamma_2(a) : \begin{pmatrix} 1 \\ x \\ \vdots \\ x^r y^s \end{pmatrix} \longmapsto \begin{pmatrix} 1 \\ a^2 x \\ \vdots \\ a^{2r+s} x^r y^s \end{pmatrix} = \begin{pmatrix} 1 & 0 & ... & 0 \\ 0 & a^2 & ... & \vdots \\ \vdots & \ddots & & 0 \\ 0 & ... & 0 & a^{2r+s} \end{pmatrix} \begin{pmatrix} 1 \\ x \\ \vdots \\ x^r y^s \end{pmatrix},$$

and

$$\gamma_3 : \begin{pmatrix} 1 \\ x \\ \vdots \\ x^r y^s \end{pmatrix} \longmapsto \begin{pmatrix} 1 \\ x+1 \\ \vdots \\ (x+1)^r y^s \end{pmatrix} = \begin{pmatrix} 1 & 0 & ... & 0 \\ 1 & 1 & ... & \vdots \\ \vdots & \ddots & & 0 \\ 0 & ... & r & 1 \end{pmatrix} \begin{pmatrix} 1 \\ x \\ \vdots \\ x^r y^s \end{pmatrix},$$

where the non-zero terms in bottom row of the matrix representation of γ_3 are in the last $r+1$ row entries and consist of the binomial coefficients $\frac{r!}{(r-j)!j!}$, $0 \leq j \leq r$. Therefore, the group generated by these matrices is lower-triangular, hence solvable. $\square$

Example 19. *Let $F = GF(p^2)$ and let $F_0 = GF(p)$.*

The automorphism group $G = Aut_F(C)$ is a central 2-fold cover of $PGL(2,p)$ andwe have a short exact sequence,

$$1 \to Z \to G \xrightarrow{\tau} PGL_2(p) \to 1, \tag{8}$$

where Z denotes the subgroup of G generated by the hyperelliptic involution (which coincides with the center of G), by Göb [G]. The group G has order $2|PGL(2,p)| = 2p(p^2-1)$. The following transformations generate G:

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

where $a \in F^\times$ is a primitive $2(p-1)-st$ root of unity.

Conjecture 20. *Let $P_1 = (1:0:1)$ and fix some $P_2 \in C(F) - C(F_0)$. The set of rational points $C(F)$ decomposes into a disjoint union*

$$C_1 = C(F_0) = G \cdot P_1, \qquad C_2 = C(F) - C(F_0) = G \cdot P_2,$$

with $|C_1| = p+1$ and $|C_2| = 2p(p-1)$.

This and Lemma 16 imply every point in $C(F)$ is ramified for the covering $C \to C/G$.

Some of this conjecture can be proven. Let $P_1 = (1 : 0 : 1)$ and let H_1 be its stabilizer in G. A counting argument shows that H_1 is a solvable group of order $2p(p-1)$ generated by γ_1, $\gamma_2(a)$, and γ_3. As a consequence, $|C_1| = |G \cdot P_1| = |G|/|H_1| = p+1$

Using $H_1 = \langle \gamma_1, \gamma_2, \gamma_3 \rangle$ and the explicit expressions for the γ_i, it can be checked directly that no $g \in H_1$, $g \neq 1$, fixes any $P \in C_2$. Therefore, $H_1 \cap H_2 = \{1\}$.

Assuming the conjecture, the stabilizer H_2 of P_2 has order $p+1$.

This and $|G| = |H_1| \cdot |H_2|$ implies $G = H_1 \cdot H_2$. In other words, H_2 is a complement of H_1 in G. (As sets, $G/H_1 \cong PGL_2(p)/B \cong \mathbb{P}^1(F_0)$.)

In fact, if B denotes the (Borel) upper-triangular subgroup of $PGL(2,p)$ then $H_1 = \tau^{-1}(B)$. Since B is solvable and any abelian cover of a solvable group is solvable, H_1 is solvable. Since B is not normal in $PGL_2(p)$, H_1 is not normal in G.

In either of these examples, the action of H_1 on the co-tangent spaces, as described in [JK], is basically the same.

The differentials on $y^2 - x^p + x = 0$ satisfy $2ydy + dx = 0$, so the action on the co-tangent space of C at P_1, $T_{P_1}(C)^*$, is determined by

$$\gamma_1 : dx \longmapsto -dx, \quad \gamma_2 : dx \longmapsto a^2 dx, \quad \gamma_3 : dx \longmapsto dx.$$

This defines a character $\psi_1 = \psi_{P_i}$ of H_1 acting on $T_{P_1}(C)^*$. The characters ψ_P, for $P \in C_1$ are given in terms of this one, since the stabilizer G_P is conjugate to H_1. Therefore, at least in principle, we can compute the constituent Γ_1 of the ramification module,

$$\Gamma_1 = \sum_{P \in G \cdot P_1} Ind_{G_P}^G \left(\sum_{\ell=1}^{e_P - 1} \ell \psi_P^\ell \right) = \sum_{P \in C_1} Ind_{G_P}^G \left(\sum_{\ell=1}^{e_P - 1} \ell \psi_P^\ell \right).$$

We have

$$\Gamma_G = \Gamma_1 + \Gamma_2,$$

wharever Γ_2 is.

4.4.2 Examples

These examples were computed using a program written by D. Joyner in [MAGMA], version 2.10, and Brauer character tables in [Gap], version 4.4.

Example 21. *Let $F = GF(7)$ and let C denote the curves 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 $\overline{F}$, $Aut_{\overline{F}}(C)/center \cong PGL_2(\overline{F})$, by [G], Theorem 1.) The following transformations are elements of $Aut_F(C)$:

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

There are 8 F-rational points:

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

The automorphism group acts transitively on $C(F)$. Consider the projection $C \to \mathbb{P}^1$ defined by $\phi(x,y) = x$. The map ϕ is ramified at every point in $C(F)$ and at no others (Proposition 4.1, [W]).

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

It is known (Proposition VI.4.1, [St]) 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

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

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* H_1 *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 $g \in H_1$*.*

Let P *denote the permutation group of this code. It a group of order* 42*. However, it is not isomorphic to* H_1*. 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?

MAGMA 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*,* γ_2 *with* $a = 2$ *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 (both in GAP and MAGMA)*

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. Accoding 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 H_1 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 $1, a, a^2, b, b^3$. The matrices of the representation ρ of H_1 acting on $L(D)$ are

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

This is not a semisimple representation, but it is solvable. In particular, H_1 is solvable.

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

Remark 2. *Similar statements hold if we replace $D = 5P_1$ by $D = mP_1$, $m = 4, 5, ..., 9$. However, when $m = 10$, the code $C(D, S)$ has permutation group S_7. In this case, the analogous homomorphism $\psi : G \to P$ is injective.*

Example 22. *Let C be the curve above but now over $F = GF(7^2)$. The automorphism group $G = Aut_F(C)$ is a central 2-fold cover of $PGL(2, 7)$: we have a short exact sequence,*

$$1 \to Z \to G \to PGL(2, 7) \to 1,$$

where Z denotes the center (containing the hyperelliptic involution of C) of G. So G has 672 elements. There are two orbits, O_1 and O_2, of the group G acting on $C(F)$. The orbit O_1 consists of all 8 of the $GF(7)$-rational points on C and the orbit $)_2$ cnsists of the remaining 84 points in $C(F) - O_1$. The stabilizer of any point in O_1 has size $|G|/|O_1| = 84$ and stabilizer of any point in O_2 has size $|G|/|O_2| = 8$. Let D be the simple effective divisor whose support is O_1. This divisor has degree 8.

Let $\rho = \rho_m : G \to Aut_F(L(mD))$ denote the natural action of G on $L(D)$. Using MAGMA, we can compute the matrices $\rho(g_i)$, for some complete set of representatives of the conjugacy classes of G, $G_* = \{g_1, ..., g_k\}$, with respect to the basis of $L(D)$ given by MAGMA. Using GAP's Brauer tables, we can use these matrix computations to determine how the semi-simpliflication of ρ decomposes.

We have

$$L(D) = \text{span}\{\frac{x^3y}{x^6-1}, \frac{x^2y}{x^6-1}, \frac{xy}{x^6-1}, \frac{y}{x^6-1}, \frac{y}{x^7-x}, 1\}.$$

Using the **SmallGroups** *library in MAGMA and GAP, we know G has order 672 and type 1043. This enables us to enter the group into GAP. The Brauer table of G can be obtained from GAP using the following commands:*

```
irr:=IrreducibleRepresentations(G,GF(49));
brvals := List(irr,chi-> List(ConjugacyClasses(G),
            c->BrauerCharacterValue(Image(chi, Representative(c)))));
```

GAP returns the Brauer table of G over F as

	$1a$	$2a$	$12b$	$12a$	$3a$	$6a$	$4b$	$4a$	$1a$	$2a$	$2b$	$2c$	$8b$	$8a$	$4c$	$4d$	$8d$	$8c$
χ_{1a}	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
χ_{1b}	1	-1	$-i$	i	1	-1	$-i$	i	1	-1	1	-1	$-i$	i	1	-1	$-i$	i
χ_{1c}	1	-1	i	$-i$	1	-1	i	$-i$	1	-1	1	-1	i	$-i$	1	-1	i	$-i$
χ_{1d}	1	1	-1	-1	1	1	-1	-1	1	1	1	1	-1	-1	1	1	-1	-1
χ_{3a}	3	-3	$-2i$	$2i$	0	0	i	$-i$	?	?	-1	1	$-a$	a	1	-1	c	$-c$
χ_{3b}	3	3	-2	-2	0	0	1	1	?	?	-1	-1	$-b$	$-b$	1	1	$-d$	$-d$
χ_{3c}	3	3	2	2	0	0	-1	-1	?	?	-1	-1	b	b	1	1	d	d
χ_{3d}	3	-3	$2i$	$-2i$	0	0	$-i$	i	?	?	-1	1	a	$-a$	1	-1	$-c$	c
χ_{5a}	5	5	-1	-1	-1	-1	-1	-1	?	?	1	1	$-b$	$-b$	-1	-1	$-d$	$-d$
χ_{5b}	5	5	1	1	-1	-1	1	1	?	?	1	1	b	b	-1	-1	d	d
χ_{5c}	5	-5	$-i$	i	-1	1	$-i$	i	?	?	1	-1	$-a$	a	-1	1	c	$-c$
χ_{5d}	5	-5	i	$-i$	-1	1	i	$-i$	?	?	1	-1	a	$-a$	-1	1	$-c$	c
χ_{7a}	7	7	1	1	1	1	1	1	?	?	-1	-1	-1	-1	-1	-1	-1	-1
χ_{7b}	7	-7	i	$-i$	1	-1	i	$-i$	?	?	-1	1	$-i$	i	-1	1	$-i$	i
χ_{7c}	7	7	-1	-1	1	1	-1	-1	?	?	-1	-1	1	1	-1	-1	1	1
χ_{7d}	7	-7	$-i$	i	1	-1	$-i$	i	?	?	-1	1	i	$-i$	-1	1	i	$-i$

where $a = \zeta_8 + \zeta_8^2 + \zeta_8^3$, $b = 1 + \zeta_8 - \zeta_8^3$, $c = \zeta_8 - \zeta_8^2 + \zeta_8^3$, $d = 1 - \zeta_8 + \zeta_8^3$, *and "?" means "fail" (i.e., it corresponds to an irregular class). Using this table, we can show that*

$$\operatorname{tr} \rho = \chi_1 + \chi_2,$$

where χ_1 *is the trivial character and* $\chi_2 = \chi_{5c}$ *or* $= \chi_{5d}$.

Example 23. *Let* $F = GF(25) = GF(5)(\alpha)$, *where* α *has splitting polynomial* $x^2 - x + 2$, *and let* C *denote the curve defined by*

$$y^2 = x^5 - x.$$

This has genus 2. *The automorphism group* $G = Aut_F(C)$ *is a central 2-fold cover of* $S_5 \cong PGL(2,5)$: *we have a short exact sequence,*

$$1 \to Z \to G \to S_5 \to 1,$$

where Z *denotes the center (containing the hyperelliptic involution of* C*) of* G. *Let* O *be the orbit of the group* G *acting on the point at infinity*[8] *in* $C(F)$ *and let* D *be the simple effective divisor whose support is* O. *This divisor has degree* 6.

Let $\rho = \rho_m : G \to Aut_F(L(mD))$ *denote the natural action of* G *on* $L(D)$. *Using MAGMA, for small values of* m, *we can compute this matrix representation with respect to the basis of* $L(mD)$ *given by MAGMA. Using the* **SmallGroups** *library, we see that* G *has order* 240 *and type* 90.

The character table of G *over* $\mathbb{C}$ *is given, according to MAGMA, by*

[8]MAGMA views the curve as embedded in a weighted projective space, with weights 1, 3, and 1, in which the point at infinity is nonsingular.

Class	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*
Size	*1*	*1*	*20*	*20*	*30*	*24*	*20*	*20*	*20*	*30*	*30*	*24*
Order	*1*	*2*	*2*	*3*	*4*	*5*	*6*	*6*	*6*	*8*	*8*	*10*
$p = 5$	*1*	*2*	*3*	*4*	*5*	*1*	*9*	*8*	*7*	*11*	*10*	*2*
χ_1	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*
χ_2	*1*	*1*	*-1*	*1*	*1*	*1*	*-1*	*1*	*-1*	*-1*	*-1*	*1*
χ_3	*4*	*-4*	*0*	*1*	*0*	*-1*	*-1-2ω*	*-1*	*1+2ω*	*0*	*0*	*1*
χ_4	*4*	*-4*	*0*	*1*	*0*	*-1*	*1+2ω*	*-1*	*-1-2ω*	*0*	*0*	*1*
χ_5	*4*	*4*	*-2*	*1*	*0*	*-1*	*1*	*1*	*1*	*0*	*0*	*-1*
χ_6	*4*	*4*	*2*	*1*	*0*	*-1*	*-1*	*1*	*-1*	*0*	*0*	*-1*
χ_7	*4*	*-4*	*0*	*-2*	*0*	*-1*	*0*	*2*	*0*	*0*	*0*	*1*
χ_8	*5*	*5*	*1*	*-1*	*1*	*0*	*1*	*-1*	*1*	*-1*	*-1*	*0*
χ_9	*5*	*5*	*-1*	*-1*	*1*	*0*	*-1*	*-1*	*-1*	*1*	*1*	*0*
χ_{10}	*6*	*6*	*0*	*0*	*-2*	*1*	*0*	*0*	*0*	*0*	*0*	*1*
χ_{11}	*6*	*-6*	*0*	*0*	*0*	*1*	*0*	*0*	*0*	z	$-z$	*-1*
χ_{12}	*6*	*-6*	*0*	*0*	*0*	*1*	*0*	*0*	*0*	$-z$	z	*-1*

where ω denotes a cube root of unity and $z \neq 0$ will be unimportant for our example. GAP returns the Brauer table of G over F as

	$1a$	$6b$	$2a$	$3a$	$6a$	$1a$	$4a$	$8b$	$2b$	$8a$	$6c$	$2b$
χ_{1a}	1	1	1	1	1	1	1	1	1	1	1	1
χ_{1b}	1	-1	-1	1	-1	1	1	-1	1	-1	1	1
χ_{2a}	2	$-a$	0	-1	a	?	0	$-b$	?	b	1	-2
χ_{2b}	2	a	0	-1	$-a$	?	0	b	?	$-b$	1	-2
χ_{3a}	3	-2	1	0	-2	?	-1	-1	?	-1	0	3
χ_{3b}	3	2	-1	0	2	?	-1	1	?	1	0	3
χ_{4a}	4	$-a$	0	1	a	?	0	0	?	0	-1	-4
χ_{4b}	4	a	0	1	$-a$	?	0	0	?	0	-1	-4
χ_{5a}	5	1	1	-1	1	?	1	-1	?	-1	-1	5
χ_{5b}	5	-1	-1	-1	-1	?	1	1	?	1	-1	5

where $a = \zeta_3 - \zeta_3^2$, $b = \zeta_8 + \zeta_8^3$. Note that the conjugacy classes of MAGMA and GAP are in different order.

Case $m = 1$.

The F-vector space $L(D)$ is 5-dimensional. We can compute $\rho(g)$, for representatives of each of the 12 conjugacy classes of G. It turns out that all but 2 of these matrices are semi-simple - for those 2 classes whose order is not prime to the characteristic, the matrix is merely solvable.

If $G_* = \{\gamma_1 = \{1\}, \gamma_2, ..., \gamma_{12}\}$ are the conjugacy classes of G then there are representatives $g_i \in \gamma_i$, $1 \leq i \leq 12$, such that the following table holds.

element	*characteristic polynomial*	*Brauer char.*	*trace*
$g_1 = 1$	$(x+4)^5$	*5*	*0*
g_2	$(x+1)^4(x+4)$	*-3*	*2*
g_3	$(x+1)^2(x+4)^3$	*1*	*1*
g_4	$(x+\alpha^4)(x+\alpha^{20}(x+4)^3$	*2*	*2*
g_5	$(x+2)^2(x+3)^2(x+4)$	*1*	*1*
g_6	$(x+4)^5$	—	*0*
g_7	$(x+\alpha^{16})(x+\alpha^{20}(x+1)(x+4)^2$	$-\zeta-1$	α^{10}
g_8	$(x+\alpha^8)(x+\alpha^{16}(x+1)(x+4)^2$	*0*	*0*
g_9	$(x+\alpha^4)(x+\alpha^8(x+1)(x+4)^2$	$\zeta-2$	α^2
g_{10}	$(x+\alpha^3)(x+\alpha^9(x+\alpha^{15})(x+\alpha^{21}(x+4)$	1	1
g_{11}	$(x+\alpha^3)(x+\alpha^9(x+\alpha^{15})(x+\alpha^{21}(x+4)$	1	1
g_{12}	$(x+1)^4(x+4)$	—	*2*

where $\zeta \in \mathbb{C}^\times$ is a 24-th root of unity corresponding to α via the identification in [Se], chapter 18. Note that since g_6 and g_{12} have orders divisible by the characteristic of the field F, the Brauer character at their classes is undefined. From the matrix values of the $\rho(g)$ ($g \in G$, which we omit), we conclude that ρ contains the trivial representation as a subrepresentation, so $\rho = 1 \oplus \sigma$, where σ is some 4-dimensional subrepresentation. From the tables, we conclude that the Brauer character of ρ is either equal to $\chi_{1a} + \chi_{4a}$ or $\chi_{1a} + \chi_{4b}$. (Which one depends on which root of $x^2 - x + 2 = 0$ is chosen for F and which cube root ω is chosen for the characters of G). In either case, this implies σ is irreducible and so, in this example, ρ is semisimple.

Case $m = 2$.

The F-vector space $L(2D)$ is 11-dimensional.

Class	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8	γ_9	γ_{10}	γ_{11}	γ_{12}
trace	1	3	1	2	4	1	α^{10}	0	α^2	1	1	3
Brauer char.	11	3	1	2	-1	*NA*		*0*				*NA*

The blank values of the Brauer character simply indicates that those liftings weren't computed.

Based on this, one can guess that ρ_{ss} decomposes as $\chi_{1a} + \chi_{3a} + \chi_{3b} + \chi_{4a}$ or $\chi_{1a} + \chi_{3a} + \chi_{3b} + \chi_{4b}$.

Case $m > 2$: Based on the data above and for the cases $m = 3, 4, 5$, which we omit, we conjecture: there is a lifting θ (see Appendix below) for which

$$\operatorname{tr} \rho_m = \begin{cases} \chi_{1a} + \chi_{4a} + k(\chi_{3a} + \chi_{3b}) + (k-1)(\chi_{4a} + \chi_{2b}), & m = 2k \text{ even}, \\ \chi_{1a} + \chi_{4a} + k(\chi_{3a} + \chi_{3b}) + k(\chi_{4a} + \chi_{2b}), & m = 2k+1 \text{ odd}. \end{cases}$$

5 Appendix: Representation-theoretic background

We give an extremely brief and incomplete sketch. See for example Serre [Se] for details.

Let G be a finite group, F a field. A finite-dimensional F-vector space V is a **modular representation** of G over F or a (left) $F[G]$**-module** if there is a homomorphism $\rho : G \to Aut_F(V)$. When $F = \mathbb{C}$ we drop the adjective "modular". We say V is **irreducible** or **simple** if there is no non-zero proper subspace V' of V which is G-invariant.

Example: Let $G = C_2 = \{1, \epsilon\}$, the cyclic group of order 2. This acts on $V = F^2$ by $1(x, y) = (x, y)$ and $\epsilon(x, y) = (y, x)$, for $(x, y) \in V$. It is not irreducible since $V' = \{(x, x)\}$ is G-invariant.

Mascke's Theorem: If F is algebraically closd and either $\operatorname{char}(F) = 0$ or $\operatorname{char}(F) = p$ does not divide G then V is semi-simple (i.e., for all $g \in G$, $\rho(g)$ is conjugate to a block-diagonal matrix).

We say a representation (ρ, V) is **equivalent** to (ρ', V') if there is an isomorphism (of F-vector spaces) $A : V \to V'$ such that, for all $v \in V$ and all $g \in G$, $\rho(g)Av = A\rho(g)v$. Up to equivalence, each semi-simple representation decomposes into a direct sum of irreducibles.

If ρ is a representation of G then the **character** of ρ is the function $\operatorname{tr} \rho : G \to F$. Since $\operatorname{tr}(A^{-1}BA) = \operatorname{tr}(B)$, $\operatorname{tr}\rho$ is constant on each conjugacy class. If

$$G_* = \{\gamma = \{x^{-1}gx \mid x \in G\}\}$$

denotes the set of conjugacy classes of G then $\operatorname{tr} \rho : G_* \to F$. Let G^* denote the set of equivalence classes of irreducible representations of G.

Fact: $|G_*| = |G^*|$.

Remark: If $G = S_n$ then there is a *natural* bijection between G_* and G^*. In general, there isn't one (known).

Example: Let G be a finite abelian group. Then $G_* = G$ and every irreducible representation of G is 1-dimensional. Once you fix a decomposition of G into cyclics (by the fundamental theorem of abelian groups), there is a natural bijection between G_* and G^*.

Let

$$(\chi, \chi') = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi'(g)}.$$

This is the **Schur inner product**.

If χ is a character on a subgroup H of G then the **induced character** is the character

$$Ind_H^G(\chi)(x) = \sum_{g \in G} \chi^0(g^{-1}xg),$$

where $\chi^0(x) = \chi(x)$ if $x \in H$ and $= 0$ otherwise.

Schur-Brauer Theorem: Assume F is algebraically closed and either characteristic 0 or $\text{char}(F) = p$ does not divide G. Then the set G^* is orthonormal with respect to the Schur inner product and spans the vector space of all class functions on G. (If either "algebraically closed" or the characteristic condition are dropped then the result can be false.)

Example: Let $G = C_2 \times C_2 = \{1, \alpha, \beta, \alpha\beta\}$. This group has character table

	1	α	β	$\alpha\beta$
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1

It is easy to check that the rows are orthogonal, as predicted by the Schur-Braur Theorem.

If (ρ, V) is a representation of G, let $[V]$ denote the equivalence class of V. Let $R(G)$ denote the Grothendieck group of all formal finite sums $\sum_i a_i[V_i]$.

Fact: $R(G) \cong \mathbb{Z}[G^*]$.

Assume now that F is an algebraically closed field of characteristic p. We call a class of G a *p-regular* conjugacy class if p does not divide the order of any of its elements. Otherwise, we call the class *irregular*. Let $G_{*,p}$ denote the collection of p-regular conjugacy classes. Let m denote the least

common multiple of all the orders of the elements in $G_{*,p}$. There is a natural isomorphism between the group of mth roots of unity of F and those of $\mathbb{C}$, $\theta : \mu_m(F) \to \mu_m(\mathbb{C})$, which we call a **lifting**. Let ρ be a finite dimensional F-representation of G, If p divides $|G|$ and g is an element of a p-regular class then then it is known that $\rho(g)$ is diagonalizable. Its eigenvalues may be lifted to $\mathbb{C}$ via θ. The trace of the resulting diagonal matrix is called the **Brauer character** (or modular character) of ρ at g.
Brauer's Theorem: The irreducible Brauer characters form a basis of the complex vector space of class functions on $G_{*,p}$.

6 Appendix: MAGMA code

```
rho_of_g:=function(f,i0,j0,m0)
 // Given is:
 //  1. f is in Poly<x>:=PolynomialRing(F), F=GF(p)
 //  2. divisor D is a G-equivariant divisor of C = HyperellipticCurve(f)
 //      in Div = DivisorGroup(C) given by G(Pt0), where
 //      i0 is position in Pts=Places(C,1) and
 //      Pt0=Pts[i0]
 //  3. g = j0-th element of G = AutomorphismGroup(C)
 //  4. m0 is multiple of D used
 //
 F:=ConstantField(FieldOfFractions(Parent(f)));
 deg:=Degree(f);
 C:=HyperellipticCurve(f);
 K<xx,yy>:=FunctionField(C);
 G, m, A := AutomorphismGroup(C);
 G_list:=[g : g in G];
//G_list_short:=[G_list[i] : i in [1..20]];
//print G_list_short;
 Pts:=Points(C,0);
//Pts:=Places(C,1); //in char p

 Div:=DivisorGroup(C);
 orbit:={};
 for k0 in [1..#G_list] do
  g0:=G_list[k0];
  orbit:=orbit join {m(g0)(Pts[i0])};
 end for;
 I:=SetToIndexedSet(orbit);
 D0:=&+[Divisor(I[i]) : i in [1..#I]];
 //computed invariant divisor

 g0:=G_list[j0];
 FF3<X,Y,Z> := FieldOfFractions(CoordinateRing(Ambient(C)));
 map_g0:= hom< FF3->FF3 | DefiningPolynomials(m(g0)) > ;

 D:=Div!D0;
 B:=RiemannRochBasis(m0*D);
 Bnew:=[];

 Poly2:=PolynomialRing(FF3,2);
 FF5<xx,yy>:=FieldOfFractions(Poly2);
 if IsEven(deg) then wt:=Floor(deg/2); else wt:=Floor((deg+1)/2); end if;
 h:=hom<K->FF3 | [X/Z,Y/Z^wt]>;
 for b in B do
  Bnew:=Bnew cat [h(b)];
 end for;

 Bnew0:=[];
 for b in Bnew do
  Bnew0:=Bnew0 cat [map_g0(b)];
 end for;
 // computing the matrix of coeffs
```

```
 repeat
  repeat
  aa:=[];
  L:=[];
  count:=0;
  denoms:=[Denominator(b) : b in Bnew0] cat [Denominator(b) : b in Bnew];
  repeat
   if Characteristic(F) eq 0 then
     pp:=[Random([1..100]),Random([1..100]),Random([1..100])];
     else pp:=[Random(F),Random(F),Random(F)];
   end if;
   if Evaluate(&*denoms,pp) ne 0 then
    L:=L cat [pp];
    count:=count+1;
   end if;
  until (count gt #B-1);
  // All s we care about are defined on pts of L
  for j in [1..#Bnew] do
   if Bnew[j] eq 1 then
    aa[j]:=[1 : i in [1..#B]];
   else
    aa[j]:=[Evaluate(Numerator(Bnew[j]),L[i])/Evaluate(Denominator(Bnew[j]),L[i]) : i in [1..#B]];
   end if;
  end for;
  AA:=Matrix([aa[i] : i in [1..#B]]);
  until (Determinant(AA) ne 0);
  //Determinant(A);
  row:=[];
  // computing the matrix rho
  for k in [1..#B] do
       v:=Vector([Evaluate(Numerator(Bnew0[k]),L[i])/Evaluate(Denominator(Bnew0[k]),L[i]) : i in [1..#B]]);
   row[k]:=Solution(AA,v);
  end for;
  rho_of_g0:=Matrix(row);
  until ((Determinant(rho_of_g0) ne 0) and (Order(rho_of_g0) eq Order(g0)));
 return rho_of_g0;
end function;



/*   examples

F:=CyclotomicField(4);
P<x>:=PolynomialRing(F);
f:=x^5-x;
C:=HyperellipticCurve(f);
G, m, A := AutomorphismGroup(C);
IdentifyGroup(G);
IdentifyGroup(G/Center(G));
CharacterTable(G);
CharacterTable(G/Center(G));
DefiningPolynomial(F);

G_list:=[g : g in G];
conj_list:=[Position(G_list, ConjugacyClasses(G)[i][3]) : i in [1..#ConjugacyClasses(G)]];
conj_list;

for j0 in conj_list do
 rho:=rho_of_g(f,1,j0,2); print rho,"  ",FactoredCharacteristicPolynomial(rho),"  ",j0,"\n";
 print JordanForm(rho),"  Jordan form \n";
 print RationalForm(rho),"  Rational form \n";
 print Trace(rho),"  = trace of rho \n";
end for;


//////////////////////////////////////////////

F:=GF(25);
P<x>:=PolynomialRing(F);
f:=x^5-x;
C:=HyperellipticCurve(f);
G, m, A := AutomorphismGroup(C);
IdentifyGroup(G);
IdentifyGroup(G/Center(G));
CharacterTable(G/Center(G));
CharacterTable(G);
```

```
G_list:=[g : g in G];
conj_list:=[Position(G_list, ConjugacyClasses(G)[i][3]) : i in [1..#ConjugacyClasses(G)]];
conj_list;
[[i,Order(G_list[i])] : i in conj_list];

for j0 in conj_list do
 rho:=rho_of_g(f,1,j0,2); print rho,"  ",FactoredCharacteristicPolynomial(rho),"  ",j0,"\n";
 print JordanForm(rho),"  Jordan form \n";
 print RationalForm(rho),"  Rational form \n";
 print Trace(rho),"  = trace of rho \n";
end for;

*/
```

References

[Bo] N. Borne, "Une formule de Riemann-Roch equivariante pour des courbes," thesis, Univ. Bordeaux, 1999. Available on the web at `http://www.dm.unibo.it/~borne/`

[Br] T. Breuer, **Characters and automorphism groups of Riemann surfaces**, London Math. Soc. Lecture Notes, 1999.

[F] W. Fulton, **Introduction to toric varieties**, Annals of Math. Studies, Princeton Univ. Press, 1993.

[Gap] The GAP Group, **GAP – Groups, Algorithms, and Programming, Version 4.3**; 2002, (`http://www.gap-system.org`).

[G] N. Göb, "Computing the Automorphism Groups of Hyperelliptic Function Fields," available at `http://front.math.ucdavis.edu/math.NT/0305284`.

[J1] D. Joyner, MAGMA code:
`http://web.usna.navy.mil/~wdj/papers/toric.mag`
GAP code:
`http://web.ew.usna.edu/~wdj/papers/toric.g`

[J2] ——, "Representations of finite groups on the Riemann-Roch space of a toric variety," preprint, available at
`http://web.ew.usna.edu/~wdj/papers.html`

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

[JK2] ——, "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, WorldScientific, 2005.

[JT] —— and W. Traves, "Representations of finite groups on Riemann-Roch spaces," 2003 preprint, available at `http://front.math.ucdavis.edu/math.AG/0210408`

[JV] —— and H. Verrill, "Notes on toric varieties," preprint, available at `http://front.math.ucdavis.edu/math.AG/0208065`

[K] B. Köck, *Galois structure of Zariski cohomology for weakly ramified covers of curves,* math.AG/0207124, available at `http://front.math.ucdavis.edu/`

[Ks] A. Ksir, "Dimensions of Prym varieties," Inter. J. Math. and Math. Sci. 26(2001)107-116.

[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/`)

[Se] J.-P. Serre, **Linear representations of finite groups**, Springer-Verlag, 1977.

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

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