The Riemann-Roch problem for divisors on two classes of surfaces

Hamish Ivey-Law

hlaw@iml.univ-mrs.fr

Institute de Mathématiques de Luminy,
Université d'Aix-Marseille

School of Mathematics and Statistics,
University of Sydney

Les Journées Codage et Cryptographie,
Dinard 2012

Introduction

- Given a divisor D on a curve C, the Riemann-Roch problem for D is the problem of calculating the dimension and determining a basis for the space of functions $L(C, nD)$ in terms of n.
- We will consider the analogous problem on certain classes of surfaces: Given a formal linear combination $mD_1 + nD_2$ of curves on a surface X, we calculate the dimension and determine a basis of the space of functions $H^0(X, mD_1 + nD_2)$ in terms of m and n.
- We consider the two cases: $X = C \times C$ and $X = \mathrm{Sym}^2(C)$ where C is a hyperelliptic curve of genus $g \geqslant 2$.

Definitions: Square of the curve

- k a field of characteristic not 2.
- C a hyperelliptic curve of genus $g \geqslant 2$.
- $C^2 = C \times C$ the square of C.
- $D_\infty = 2(\infty)$ or $D_\infty = (\infty^+) + (\infty^-)$ depending on whether C has one or two points at infinity.
- $\infty \in C(\overline{k})$
- $V_\infty = \{\infty\} \times C$ the vertical embedding of C in C^2.
- $H_\infty = C \times \{\infty\}$ the horizontal embedding of C in C^2.
- $F = 2(V_\infty + H_\infty)$.
- Δ and ∇ the diagonal and antidiagonal embeddings of C in C^2; let D_∇ be the image of D_∞ on ∇.

Definitions: Symmetric square of the curve

- $S = C^2 / \langle \sigma \rangle$ the symmetric square of C and

$$\pi : C^2 \to S$$

  is the quotient map.
- $\Delta_S = \pi(\Delta)$,
- $\nabla_S = \pi(\nabla)$ and
- $\Theta_S = \pi(V_\infty) = \pi(H_\infty)$ are the (scheme-theoretic) images under the quotient map.

Subgroups of $\mathrm{Div}(C^2)$ and $\mathrm{Div}(S)$

Let m and r be non-negative integers.

- V_∞, H_∞ and ∇ are linearly independent in $\mathrm{Div}(C^2)$.
- We will consider the divisors of the form $mF + r\nabla$ in $\mathrm{Div}(C^2)$ (where $F = 2(V_\infty + H_\infty)$).
- Divisors of this form don't span $\mathrm{Div}(C^2)$.
- There is a relation

$$F \sim \Delta + \nabla$$

coming from the function $x_1 - x_2$ on C^2 where $k(C^2) = k(x_1, y_1, x_2, y_2)$.

Subgroups of $\mathrm{Div}(C^2)$ and $\mathrm{Div}(S)$

Let m and r be non-negative integers.

- Θ_S and ∇_S are linearly independent in $\mathrm{Div}(S)$.
- We will consider divisors of the form $2m\Theta_S + r\nabla_S$ in $\mathrm{Div}(S)$.
- Divisors of this form don't span $\mathrm{Div}(S)$.
- There is a relation

$$4\Theta_S \sim 2\Delta_S + 2\nabla_S$$

coming from the function $(x_1 - x_2)^2$ on S.

Fundamental exact sequence

Throughout we fix $\gamma = g - 1$.
Let m and r be non-negative integers. Then

$$\begin{aligned} 0 \to \mathscr{O}_{C^2}(mF + (r-1)\nabla) \\ \to \mathscr{O}_{C^2}(mF + r\nabla) \\ \to \mathscr{O}_{\nabla}((2m - \gamma r)D_{\nabla}) \to 0 \end{aligned}$$

is an exact sequence (because $\mathscr{O}_{C^2}(mF + r\nabla) \otimes \mathscr{O}_{\nabla} \cong \mathscr{O}_{\nabla}((2m - \gamma r)D_{\nabla})$).

We thus obtain a long exact sequence of cohomology

$$\begin{aligned}
0 &\to H^0(C^2, mF + (r-1)\nabla) \\
&\to H^0(C^2, mF + r\nabla) \\
&\to H^0(\nabla, (2m - \gamma r)D_\nabla) \\
&\to H^1(C^2, mF + (r-1)\nabla) \\
&\to H^1(C^2, mF + r\nabla) \\
&\to H^1(\nabla, (2m - \gamma r)D_\nabla) \to \cdots
\end{aligned}$$

The easy cases

- If $2m - \gamma r < 0$, then $H^0(\nabla, (2m - \gamma r)D_\nabla) = 0$, so

$$H^0(C^2, mF + (r-1)\nabla) \cong H^0(C^2, mF + r\nabla).$$

- If $2m - \gamma r > 0$, then $H^1(C^2, mF + (r-1)\nabla) = 0$, so

$$\begin{aligned} &H^0(C^2, mF + r\nabla) \\ &\qquad \cong H^0(C^2, mF + (r-1)\nabla) \oplus H^0(\nabla, (2m - \gamma r)D_\nabla). \end{aligned}$$

- What happens when $2m - \gamma r = 0$?

The split long exact sequence

Suppose $2m - \gamma r = 0$.

- $H^0(\nabla, (2m - \gamma r)D_\nabla) = H^0(\nabla, \mathscr{O}_\nabla)$ has dimension 1.
- $H^1(C^2, mF + (r-1)\nabla)$ is not necessarily zero.
- We can nevertheless show that that

$$H^0(C^2, mF + r\nabla) \setminus H^0(C^2, mF + (r-1)\nabla) \neq \emptyset$$

by constructing an element explicitly.

The split long exact sequence

So when $2m - \gamma r = 0$ we still get an exact sequence

$$0 \to H^0(C^2, mF+(r-1)\nabla) \to H^0(C^2, mF+r\nabla) \to H^0(\nabla, \mathscr{O}_\nabla) \to 0$$

because the coboundary map

$$H^0(\nabla, \mathscr{O}_\nabla) \to H^1(C^2, mF + (r-1)\nabla)$$

is zero.

Structure of $H^0(C^2, mF + r\nabla)$

Theorem

Let m and r be an integers satisfying $m > \gamma$ and $r \geqslant 0$. We have

$$H^0(C^2, mF + r\nabla) \cong H^0(C^2, mF) \oplus \bigoplus_{i=1}^{r} H^0(\nabla, (2m - \gamma i)D_\nabla).$$

Corollary

$$h^0(C^2, mF + r\nabla)$$
$$= \begin{cases} (2m-\gamma)^2 + 4mr - \gamma r(r+2) & \textit{if } \gamma < 2m - \gamma r, \\ (2m-\gamma)^2 + 4mr - \gamma r(r+1) - 2m + g & \textit{if } 0 < 2m - \gamma r \leqslant \gamma, \\ (2m-\gamma)^2 + 2m(r-2) + g + 1 & \textit{if } 2m - \gamma r = 0, \textit{ and} \\ h^0(C^2, mF + \left\lfloor \frac{2m}{\gamma} \right\rfloor \nabla) & \textit{if } 2m - \gamma r < 0. \end{cases}$$

Structure of $H^0(S, 2m\Theta_S + r\nabla_S)$

Theorem

Let m be an integer with $m > \gamma$. Then for all integers $r \geqslant 0$,

$$H^0(S, 2m\Theta_S + r\nabla_S) \cong H^0(S, 2m\Theta_S) \oplus \bigoplus_{i=1}^{r} H^0(\mathbb{P}^1, (2m - \gamma i)(\infty)).$$

Dimension of $H^0(S, 2m\Theta_S + r\nabla_S)$

Corollary

If $2m - \gamma r \geqslant 0$, *then*

$$h^0(S, 2m\Theta_S + r\nabla_S)$$
$$= \frac{(2m-\gamma)(2m-\gamma+1)}{2} + r(2m+1) - \gamma\frac{r(r+1)}{2}.$$

Otherwise

$$h^0(S, 2m\Theta_s + r\nabla) = h^0(S, 2m\Theta_S + \left\lfloor \frac{2m}{\gamma} \right\rfloor \nabla).$$

$k[D_4]$-module structure

Goal: an explicit basis for $H^0(S, 2m\Theta_S + r\nabla_S)$.

Proposition

For any divisor D on $S = C^2/\langle\sigma\rangle$,

$$H^0(S, D) \cong H^0(C^2, \pi^* D)^\sigma.$$

Since $\pi^*(2m\Theta_S + r\nabla_S) = mF + r\nabla$, we reduce to the problem of computing $H^0(C^2, mF + r\nabla)^\sigma$.

$k[D_4]$-module structure

Proposition

$$H^0(C^2, mF + r\nabla)^\sigma \cong W_{m+r,r}^{(-1)^r}$$

where $W_{m+r,r}^{(-1)^r}$ *denotes the subspace of* $H^0(C^2, (m+r)F - r\Delta)$ *on which* σ *acts by* $(-1)^r$.

This follows from the isomorphism

$$H^0(C^2, mF + r\nabla) \cong H^0(C^2, (m+r)F - r\Delta)$$

obtained from the relation $F \sim \Delta + \nabla$.

In a neighbourhood of Δ

- For any section $w \in H^0(C^2, (m+r)F)$ we can consider the formal expansion

$$w = \sum_{i=0}^{\infty} (D^{(i)} w)(0) t^i$$

  in a neighbourhood of Δ. Here $t = \frac{1}{2}(x_1 - x_2)$ is a uniformising parameter at Δ and "$D^{(i)} w = \frac{1}{i!} \frac{\partial w}{\partial t}$" is the ith Hasse derivative of w with respect to t.
- A section with valuation at least r on Δ is one for which $(D^{(i)} w)(0) = 0$ for $i = 0, \ldots, r-1$.

In a neighbourhood of Δ

- We have reduced the problem to finding a basis of $W^{(-1)^r}_{m+r,r}$.
- But

$$W^{+1}_{m+r,r} = H^0(C^2, (m+r)F - r\Delta)^\sigma$$
$$W^{-1}_{m+r,r} = (x_1 - x_2)H^0(C^2, (m+r-1)F - r\Delta)^\sigma$$

are subspaces of $H^0(C^2, (m+r)F) \cong H^0(C, (m+r)D_\infty)^{\otimes 2}$ of sections with valuation at least r on Δ.

An explicit description of the basis

- Define
$$\varphi_i : W_{m+r,0}^{(-1)^r} \to k(\Delta)$$
by sending a section $w \in W_{m+r,0}^{(-1)^r} \subset H^0(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(s))$ to $(D^{(i)}w)(0)$ (here s is of order m).
- The image lies in a finitely generated subring.
- φ_i is linear (being just a derivative and evaluation) and (after fixing bases) is given by a vector in k^u for some u (of order m^2).
- The basis we desire is simply
$$\mathrm{Ker}(\bigoplus_{i=0}^{r-1} \varphi_i) = \bigcap_{i=0}^{r-1} \mathrm{Ker}(\varphi_i)$$
where $\bigoplus_{i=0}^{r-1} \varphi_i$ is the matrix formed by the φ_i.

Projective embeddings

- If C has genus $g = 2$, we obtain the well-known embedding of J_C in $\mathbb{P}^{15}$ published by Cassels and Flynn. In the present work, this corresponds to calculating a basis of the space $H^0(S, 4\Theta_S + 4\nabla_S)$.

The Fujita conjecture

- Let X be a smooth projective variety of dimension n, let K_X be a canonical divisor on X and let H be an ample divisor on X. Then $K_X + \lambda H$ is very ample if and only if $\lambda \geqslant n + 2$.
- In 1988, Igor Reider demonstrated the Fujita conjecture in the case of surfaces.
- We can show that $K_{C^2} = \gamma F$ is a canonical divisor on C^2 and $K_S = 2\gamma\Theta_S - \Delta_S$ is a canonical divisor on S.
- Hence we can now explicitly give several new embeddings of C^2 and S.

Codes on C^2 and S

- Bases of $H^0(C^2, mF + r\nabla)$ and $H^0(S, 2m\Theta_S + r\nabla_S)$ can be used to define codes.
- The analysis of these codes is yet to be done...

Concluding remarks

There are several possible generalisations we might try:

- Similar results for elliptic curves are probably trivial to determine.
- Given a relatively explicit description of $\mathrm{End}(J_C)$ in terms of the intersection theory of the correspondences, can we find dimension formulae and explicit bases for arbitrary divisors on these surfaces? At least the Frobenius divisor in positive characteristic?
- Characteristic 2 will require new techniques.
- Higher symmetric products would allow us produce the birational maps $C^{(g)} \to J_C$ to the Jacobian, but requires a much more sophisticated theory.