Arithmetic on Jacobians of Relative Curves

Being one half of a recently defended thesis...

Hamish Ivey-Law

Supervisor: David Kohel

Co-supervisor: Claus Fieker

Institut de Mathématiques de Luminy
Université d'Aix-Marseille

School of Mathematics and Statistics
University of Sydney

22 janvier 2013

1. Divisors on relative curves
   - Khuri-Makdisi's addition algorithm
   - Relative curves and relative effective Cartier divisors
   - Criteria for normal generation
   - Tensor products and module quotients

2. Divisor arithmetic on relative Jacobians
   - Linear algebra over amenable rings
   - Arithmetic of divisors

Introduction

- Given two points x and y on the Jacobian of an algebraic curve, there are various methods to explicitly compute the sum $x + y$. For example,
  - using the Mumford representation of divisors,
  - using Hess's arithmetic method of Riemann-Roch spaces in algebraic function fields, or
  - using Khuri-Makdisi's geometric method of Riemann-Roch spaces with respect to a projective embedding of the curve.
- The goal of the first part of this work is to show that Khuri-Makdisi's approach can be generalised to the case of the Jacobian of a relative curve over an affine Noetherian base scheme.

Representing divisors on algebraic curves

- Let X be an algebraic curve.
- Fix a very ample invertible sheaf $\mathscr{L}$ on X of degree at least $2g+1$.
- An effective divisor D on X is given by a basis for the subspace $H^0(X, \mathscr{L}(-D))$ of $H^0(X, \mathscr{L})$. If $\mathscr{L}(-D)$ is generated by global sections, this represents the divisor precisely.
- The degree of $\mathscr{L}$ determines an upper bound on the divisors D that we can represent. Indeed, if

$$\deg(D) \leqslant \deg(\mathscr{L}) - (2g+1),$$

  then $\mathscr{L}(-D)$ is very ample and hence generated by its global sections.
- Let $\mathscr{M}$ be an element of $\mathrm{Pic}^0_X(k)$; so $\mathscr{M}$ is an invertible sheaf of degree 0.
  - The isomorphism class of $\mathscr{M}$ is represented by any effective divisor D of degree $\deg(\mathscr{L})$ such that $\mathscr{M} \cong \mathscr{L}(-D)$.
  - Since $\deg(\mathscr{L}) \geqslant 2g+1$, we have $\deg(\mathscr{L}^2(-D)) = \deg(\mathscr{L}) \geqslant 2g+1$ and so $\mathscr{L}^2(-D)$ is very ample.
  - We can therefore represent $\mathscr{M}$ by the space $H^0(X, \mathscr{L}^2(-D))$.

Module quotients

Let M, N and P be R-modules and let $\mu\colon M \otimes N \to P$ be a homomorphism. Let $N' \subseteq N$ and $P' \subseteq P$ be submodules. The *module quotient* of P' by N' is defined to be the R-submodule

$$(P' : N') = \{m \in M \mid \mu(m \otimes N') \subseteq P'\}$$

of M.

Khuri-Makdisi's multiplication and quotient propositions

Let X be a complete, smooth, geometrically connected curve of genus g over a field k and let $\mathscr{M}$ and $\mathscr{N}$ be invertible sheaves on X.

Proposition (Khuri-Makdisi)

Suppose $\mathscr{M}$ and $\mathscr{N}$ are each of degree at least $2g+1$. Then the canonical map

$$\mu : H^0(X, \mathscr{M}) \otimes H^0(X, \mathscr{N}) \to H^0(X, \mathscr{M} \otimes \mathscr{N})$$

is surjective.

Proposition (Khuri-Makdisi)

Suppose $\mathscr{N}$ is generated by global sections and let D be any effective divisor on X. Then we have an equality

$$H^0(X, \mathscr{M}(-D)) = (H^0(X, \mathscr{M} \otimes \mathscr{N}(-D)) : H^0(X, \mathscr{N}))$$

where the quotient is taken with respect to the map μ above.

Khuri-Makdisi's addflip algorithm

Algorithm (Khuri-Makdisi)

Let x and y be elements of $\mathrm{Pic}^0_X(k)$ given by submodules $H^0(X, \mathscr{L}^2(-D_1))$ and $H^0(X, \mathscr{L}^2(-D_2))$. The following procedure calculates a divisor E on X and a section $s \in H^0(X, \mathscr{L}^3)$ such that

$$\mathrm{div}(s) = D_1 + D_2 + E.$$

1. Multiply $H^0(X, \mathscr{L}^2(-D_1))$ and $H^0(X, \mathscr{L}^2(-D_2))$ to obtain $H^0(X, \mathscr{L}^4(-D_1 - D_2))$.
2. Calculate $H^0(X, \mathscr{L}^3(-D_1 - D_2)) = (H^0(X, \mathscr{L}^4(-D_1 - D_2)) : H^0(X, \mathscr{L}))$.
3. Choose a non-zero $s \in H^0(X, \mathscr{L}^3(-D_1 - D_2))$.
4. Multiply s and $H^0(X, \mathscr{L}^2)$ to obtain $H^0(X, \mathscr{L}^5(-D_1 - D_2 - E))$.
5. Calculate
$$H^0(X, \mathscr{L}^2(-E)) = (H^0(X, \mathscr{L}^5(-D_1 - D_2 - E)) : H^0(X, \mathscr{L}^3(-D_1 - D_2))).$$
6. Return $H^0(X, \mathscr{L}^2(-E))$ and s.

Arithmetic on a Jacobian

There is an algorithm which produces a divisor in the class of zero and an algorithm for testing whether a given divisor is zero. We will not discuss these here.

Given $x, y \in \mathrm{Pic}^0_X(k)$, Khuri-Makdisi's algorithm produces $-x - y$. We then have

- Negation: $-x = -x - 0$.
- Addition: $x + y = -(-x - y)$.
- Difference: $x - y = -(-x) - y$.
- Equality: take the difference and compare with zero.

Relative curves

We will now prove generalisations of Khuri-Makdisi's multiplication and quotient propositions for relative effective Cartier divisors on relative curves, from which it will follow that the addflip algorithm remains valid in much greater generality.

- Let S be a scheme. An S-scheme X is called a *relative curve* if it is projective and smooth of relative dimension one with geometrically connected fibres.
- We think of X/S as a family of geometrically connected, smooth, projective algebraic curves parametrised by S.

Relative effective Cartier divisors

- Let $f : X \to S$ be a relative curve. A *relative effective Cartier divisor* on X is closed subscheme $\iota : D \to X$ whose ideal sheaf is invertible such that $f \circ \iota : D \to S$ is flat.
- There is a correspondence between isomorphism classes of invertible sheaves that are flat over S and relative effective Cartier divisors.
- The restriction of a relative effective Cartier divisor on a relative curve to a geometric fibre (an algebraic curve) gives an effective divisor on that fibre.
- The Euler characteristic of an invertible sheaf on X is locally constant, hence so are the genera of the fibres and the degrees of the relative effective Cartier divisors.

Relative effective Cartier divisors

Let $X \to S$ be a relative curve.

Proposition

Let $\mathscr{F}$ be an $\mathscr{O}_X$-module which is flat over S. If $H^1(X, \mathscr{F})$ is projective, then so is $H^0(X, \mathscr{F})$.

Proposition

If $\mathscr{L}$ is a very ample sheaf on X, then $H^1(X, \mathscr{L}) = 0$. In particular, the module of global sections of a very ample sheaf is projective.

Fibres

Henceforth, we set $S = \mathrm{Spec}(R)$ for some Noetherian ring R.

- Let s be a closed point of S.
- Denote the fibre of X above s by $X_s = X \times \mathrm{Spec}(k(s))$ where $k(s)$ is the residue field at s.
- For an invertible sheaf $\mathscr{L}$ on X, denote by $\mathscr{L}_s = \rho_s^* \mathscr{L}$ the fibre of $\mathscr{L}$ over s, where $\rho_s : X_s \to X$ is the projection map.

Criteria for very ampleness

Proposition

Let X be a relative curve and let $\mathscr{L}$ be an invertible sheaf on X. Then $\mathscr{L}$ is very ample on X if and only if $\mathscr{L}_s$ is very ample on X_s for all closed points $s \in S$.

Corollary

Let X be a relative curve of genus g and let $\mathscr{L}$ be an invertible sheaf on X. If $\deg(\mathscr{L}) \geqslant 2g+1$, then $\mathscr{L}$ is very ample.

Criteria for normal generation

Let X be a scheme and let $\mathscr{L}$ be an invertible sheaf on X. Then $\mathscr{L}$ is said to be *normally generated* if it is ample and the natural map

$$H^0(X,\mathscr{L})^{\otimes n} \to H^0(X,\mathscr{L}^{\otimes n})$$

is surjective for all $n > 0$.

Proposition

Let X be a relative curve and let $\mathscr{L}$ be an invertible sheaf on X. Then $\mathscr{L}$ is normally generated if and only if it is very ample and the natural maps

$$H^0(\mathbb{P}^n,\mathscr{O}_{\mathbb{P}^n}(d)) \to H^0(X,\mathscr{L}^{\otimes d})$$

are surjective for all $d \geqslant 1$.

Proposition

Let X be a relative curve of genus g and let $\mathscr{L}$ be an invertible sheaf on X. If $\deg(\mathscr{L}) \geqslant 2g+1$, *then $\mathscr{L}$ is normally generated.*

Tensor products

Proposition (I.-L.)

Let X be a relative curve and let $\mathscr{M}$ and $\mathscr{N}$ be normally generated sheaves on X. Then

$$\mu : H^0(X, \mathscr{M}) \otimes H^0(X, \mathscr{N}) \to H^0(X, \mathscr{M} \otimes \mathscr{N})$$

is surjective.

Sketch of proof.

We obtain a commutative diagram

$$\begin{tikzcd}
H^0(\mathbb{P}^m, \mathscr{O}_{\mathbb{P}^m}(1)) \otimes H^0(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(1)) \arrow[r] \arrow[d] & H^0(X, \mathscr{M}) \otimes H^0(X, \mathscr{N}) \arrow[r] \arrow[d, "\mu"] & 0 \\
H^0(\mathbb{P}^m \times \mathbb{P}^n, \mathscr{O}_{\mathbb{P}^m \times \mathbb{P}^n}(1)) \arrow[r] & H^0(X, \mathscr{M} \otimes \mathscr{N}) \arrow[r] & 0
\end{tikzcd}$$

where all maps except μ are known to be surjective. Thus μ is surjective. □

Module quotients

Proposition (I.-L.)

Let X be a relative curve of genus g and let $\mathscr{M}$ and $\mathscr{N}$ be invertible sheaves on X, each of degree at least $2g+1$. Then for any relative effective Cartier divisor D on X of degree at most $\deg(\mathscr{M}) - (2g+1)$, we have

$$H^0(X, \mathscr{M}(-D)) = \left(H^0(X, \mathscr{M} \otimes \mathscr{N}(-D)) : H^0(X, \mathscr{N})\right).$$

Sketch of proof.

Khuri-Makdisi proved that the result holds on the fibres. We can show that tensoring by $k(s)$ and taking global sections "commute" in the sense that

$$H^0(X, \mathscr{L}) \otimes k(s) \cong H^0(X_s, \mathscr{L}_s)$$

when $\mathscr{L}$ is very ample and $s \in S$ is closed. Using properties of the module quotient, we can then "lift" Khuri-Makdisi's result from the fibres to the relative curve using Nakayama's Lemma. □

Amenable rings

Let R be a ring. We say that R is *amenable* if

- we can perform exact arithmetic on elements of R, and
- the following functions are effectively computable on projective R-modules and homomorphisms between them:
  - **Dual:** Given $\varphi : M \to N$, return the dual homomorphism $\varphi^\vee : N^\vee \to M^\vee$.
  - **Composite:** Given $\varphi : M \to N$ and $\psi : N \to P$, return the composite $\psi \circ \varphi : M \to P$.
  - **Kernel:** Given $\varphi : M \to N$, return $\kappa : K \to M$ such that $\mathrm{Ker}(\varphi) = \mathrm{Im}(\kappa)$.
  - **Common kernel:** Given $\varphi_i : M \to N$, return the common kernel $\bigcap_i \varphi_i$.
  - **Sum:** Given submodules $M_1, M_2 \subseteq M$, return $M_1 + M_2 \subseteq M$.

Examples of amenable rings:

- Finite fields, the rationals, the integers (classic).
- Dedekind domains (Bosma, Pohst, Cohen), for example the ring of integers in a number field.
- Finite semi-local rings (Howell, Storjohann), for example $\mathbb{Z}/n\mathbb{Z}$.
- Certain approximation structures for $\mathbb{Z}_p [\![u]\!]$ (Caruso, Lubicz).

The case of primary interest is that of local Artin rings, in particular quotients of discrete valuation rings.

Arithmetic of modules - Multiplication

- Let R be an amenable ring.
- Let M, N and P be finitely generated projective R-modules and let $\mu : M \otimes N \to P$ be a homomorphism.
- Given finitely generated submodules $M' \subseteq M$ and $N' \subseteq N$, evaluating the image $\mu(M' \otimes N')$ can be reduced to matrix multiplications defined with respect to the generating sets of M, N and P.

Arithmetic of modules - Quotients

Let M, N, P and μ be as in the previous slide.

Proposition (I.-L.)

Let $N' \subseteq N$ and $P' \subseteq P$ be finitely generated projective submodules and suppose P' is a direct summand of P. Let $\{g_1, \ldots, g_{n'}\}$ be a generating set for N'. Then there exists a homomorphism $\kappa : P \to R^k$ whose kernel is P' and we have

$$(P' : N') = \bigcap_{i=1}^{n'} \mathrm{Ker}(\kappa^\vee \circ \mu_{g_i}).$$

It is clear from this proposition that we can effectively calculate $(P' : N')$.

Representing divisors in general

- Fix a relative curve $f: X \to S$ where $S = \mathrm{Spec}(R)$ for an amenable ring R.
- Fix a very ample invertible sheaf $\mathscr{L}$ on X of large degree.
- The module of global sections $H^0(X, \mathscr{L})$ is projective.
- A relative effective Cartier divisor D on X is given as the set of generators of the finitely generated submodule $H^0(X, \mathscr{L}(-D))$ of $H^0(X, \mathscr{L})$.
- We can use the multiplication map

$$\mu: H^0(X, \mathscr{M}) \otimes H^0(X, \mathscr{N}) \to H^0(X, \mathscr{M} \otimes \mathscr{N})$$

  to perform arithmetic in using the module algorithms we just saw when $\mathscr{M}$ and $\mathscr{N}$ are normally generated.
- The degree of $\mathscr{L}$ determines an upper bound on the divisors D that we can represent. Indeed, if

$$\deg(D) \leqslant \deg(\mathscr{L}) - (2g + 1),$$

  then $\mathscr{L}(-D)$ is normally generated.

Representing divisor classes on a relative Jacobian

- The *Picard group*, $\mathrm{Pic}(X)$, of X is the group $H^1(X, \mathscr{O}_X^*)$ of isomorphism classes of invertible sheaves on X.
- For any S-scheme T, define

$$\mathrm{Pic}^0_X(T) = \{\mathscr{L} \in \mathrm{Pic}(X_T) \mid \deg(\mathscr{L}_t) = 0 \text{ for all } t \in T\}/f_T^* \,\mathrm{Pic}(T).$$

- Let $\mathscr{M}$ be an invertible sheaf of degree 0. As before, we can represent it by the module $H^0(X, \mathscr{L}^2(-D))$ where D is any relative effective Cartier divisor such that $\mathscr{M} \cong \mathscr{L}(-D)$.

Proposition (I.-L.)

The 'addflip' algorithm of Khuri-Makdisi is correct (mutatis mutandis) when operating on classes of relative effective Cartier divisors in $\mathrm{Pic}^0_X(S)$*, represented as above, for a relative curve* $X \to S$*.*

A note on complexity

- The algorithms of Khuri-Makdisi that we have generalised here have time complexities in $O(g^4)$ where g is the genus of the curve.
- Under reasonable assumptions about the linear algebra of modules over amenable rings, the generalised algorithms also have time complexities in $O(g^4)$.

Merci pour votre attention!

Thank you for your attention.