
Arithmetic in Picard Groups and Application to Pairings 2

GTEM Workshop on Pairings, IEM Essen

5. Mai 2009

Florian Heß

Technische Universität Berlin

Motivation

This talk is about fast arithmetic in divisor class groups of algebraic curves over finite fields for large genus.

What you do not get from this talk:

- Fast arithmetic for low genus curves optimised for use in a cryptographic system.

Some reasons why to consider this problem:

- General interest
- Useful for index calculus attacks, pairings.

Previous work

There is a long history of previous work on the **theory** and on **algorithms** for the

- Riemann-Roch problem
- arithmetic in class groups
- algebraic geometric codes
- integration of algebraic functions
- parametrisation of algebraic curves
- ...

Can roughly be divided into

- **arithmetic** methods (integral closures, ideals, ...)
- **geometric** methods (Brill-Noether method of adjoints, ...)

Previous work

Theory:

- Brill and Noether (1874, 1884),
- Dedekind and Weber (1882), F. K. Schmidt (1931).

Geometric and arithmetic algorithms for divisor class groups for $g \rightarrow \infty$:

1987	Cantor	hyperell. divclgrp	$O(g^2)$
1993	Huang, Ierardi	RR problem + divclgrp for general plane curves	$O(n^6 h(D)^6)$
1994	Volcheck	divclgrp for g. p. curves	$O(\max\{n, g\}^7)$
1998	Galbraith, Paulus, Smart	divclgrp for superell. curves	$O(n^4 g^4)$
1999	Arita	divclgrp for $C_{a,b}$ curves	$O(g^3)$

Previous work

Geometric and arithmetic algorithms for divisor class groups for $g \rightarrow \infty$ (ctd):

1999	Hess	RR problem and divclgrp for general curves	$O(g^2)$ for fixed n
2001	Khuri-Makdisi	divclgrp for general curves	$O^\sim(g^3)$
2004		with precomputation	

This and next slide $n = \min\{[F : k(x)] \mid x \in F \text{ separating}\}$.

Discussion

KM result:

- Links complexity of `divclgrp` to complexity of linear algebra over k in dimension $O^\sim(g)$.
- Probably optimal in the general case ($n \gtrsim g/2$).
- Fast linear algebra $O^\sim(g^\omega)$ with $\omega = 2.376$.

H result:

- Links complexity of `divclgrp` to complexity of polynomial arithmetic over k in degree $O(g)$.
- Probably optimal under the assumption $n = O(1)$.
- Fast polynomial arithmetic $O^\sim(g)$.

This talk: Combine both running time characteristics towards $O^\sim(gn^{\omega-1})$ with $n = O(g)$.

Divisor and ideal class groups

Let

- $x \in F$ be separating with $(x)_\infty = nP$ and $\deg(P) = 1$,
- $R = \text{Cl}(k[x], F)$.
- $n = O(g)$.

Then

- R is a Dedekind domain.
- Ideals $I \neq \{0\}$ of R are free $k[x]$ -modules of rank n and form a multiplicative monoid with cancellation law.
- $\text{Pic}(R) = (\text{group of fractional ideals}) / (\text{group of principal ideals})$.
- $\text{Pic}(R) \cong \text{Pic}^0(F)$.

Arithmetic in the ideal class group

Represent ideal classes $[I]$ by integral ideals I of small „degree“.

Basic ideal operations for integral ideals I, J :

- Simple multiplication: Compute zI for $z \in J$.
- Integral division: Compute I/J for $J|I$.

Degree reduction:

- Rz/I has small degree if $z \in I$ has degree close to that of I .
- Do not necessarily get unique reduction ... but yields bounded representation for I^{-1} and I .

When writing $z \in I$ we always mean to pick z of degree close to that of I .

Arithmetic in the ideal class group

Arithmetic operations for $[I], [J] \in \text{Pic}(R)$:

- Division: $[I][J]^{-1} = [(zI)/J]$ for $z \in J$.
- Inversion: Use division with $[I] = [R]$.
- Multiplication: Use division and inversion.

Equality test for $[I], [J] \in \text{Pic}(R)$:

- Let $[K] = [I][J]^{-1}$.
- Then $[I] = [J]$ iff $K = Rz$ for some $z \in K$ of smallest degree.

Use linear algebra over $k[x]$!

Bases, matrices and degree function

Integral basis $\omega_1, \dots, \omega_n \in R$ of R :

- $\forall z \in R : \exists$ unique $\lambda_i \in k[x]$ such that $z = \sum_i \lambda_i \omega_i$.
- Multiplication table $\lambda_{i,j,v} \in k[x]$: $\omega_i \omega_j = \sum_v \lambda_{i,j,v} \omega_v$.

Ideal basis $\alpha_i \in I$ of ideal I :

- $\forall z \in I : \exists$ unique $\lambda_i \in k[x]$ such that $z = \sum_i \lambda_i \alpha_i$.
- Basis matrix $M_I \in k[x]^{n \times n}$: $(\alpha_1, \dots, \alpha_n) = (\omega_1, \dots, \omega_n) M_I$.

Principal ideal I :

- $I = Rz$ for some $z \in I$.
- Representation matrix $M_z \in k[x]^{n \times n}$: $(z\omega_1, \dots, z\omega_n) = (\omega_1, \dots, \omega_n) M_z$.

Degree function:

- $\deg^*(z) = -v_P(z)$ for $z \in R$, $\deg^*(I) = \deg(\det(M_I))$.
- Have $\deg^*(z) = \deg^*(Rz)$, $\deg^*(x) = n$.

Bounded representations

Fix $\omega_1, \dots, \omega_n$ with successively smallest \deg^* -values and let $d = g/n$.

Theorem:

1. There is a basis α_i of I with $\deg^*(\alpha_i) \leq \deg^*(I) + 2g$ for all i .
There is α_j with $\deg^*(\alpha_j) \leq \deg^*(I) + g$.
2. Elements of $\text{Pic}(R)$ can be represented by I with $\deg^*(I) \leq g$.
3. $\deg(\lambda_{i,j,v}) \leq 4d$.
4. $\deg^*(\sum_i \lambda_i \omega_i) \leq w \Rightarrow \deg(\lambda_i) \leq w/n$ for all i .
5. $\deg^*(I) \leq w \Rightarrow$ there is a basis matrix M_I with $\deg(M_I) \leq w/n$.

Represent elements of $\text{Pic}(R)$ by integral ideals of degree $\leq g$ with $n \times n$ basis matrices of degree $\leq 3d$.

Linear algebra over polynomial rings

References: Storjohann, Villard, ...

Matrix multiplication in dimension n and degree d :

- Time $O(d^2n^3)$.

Degree reduction (function field LLL, weak Popov form):

- Let $M = (v_1, \dots, v_m) \in k[x]^{n \times m}$, r be the rank of M ,
 $d = \deg(M) = \max_i \deg(v_i)$ the maximum polynomial degree in M .
- M is reduced iff $\deg(\sum_i \lambda_i v_i) = \max_i \deg(\lambda_i v_i)$ for all $\lambda_i \in k[x]$.
- M can be transformed into reduced matrix by unimodular column operations in time $O(d^2nmr)$.

Kernel of M :

- Assume M has a basis matrix K for the $k[x]$ -column kernel with $\deg(K) \leq d$ and that $m \geq n$.
- Then such a K can be computed in time $O(d^2m^3)$.

Simple multiplication

Compute zI for $z \in R$ with $\deg^*(z) = O(g)$ and I integral ideal with $\deg^*(I) = O(g)$.

Algorithm:

- Compute representation matrix M_z of z wrt ω_i .
If $z = \sum_i \mu_i \omega_i$ then $z\omega_j = \sum_v (\sum_i \mu_i \lambda_{i,j,v}) \omega_v$.
- Multiply M_z and basis matrix of I to obtain a basis matrix of zI .

Note $\deg^*(zI) = \deg^*(z) + \deg^*(I)$.

Each step requires time $O(d^2n^3)$.

Integral division

Let I, J with $I | J$ and $\deg^*(J) = O(g)$. Compute $J I^{-1} = \{z \in R \mid zI \subseteq J\}$.

- Let $I = \sum_{j=1}^h R\beta_j$ and M_J be the basis matrix of J .
- For $z = \sum_i \lambda_i \omega_i$ and $\lambda = (\lambda_1, \dots, \lambda_n)^t \in k[x]^n$:

$$z \in J I^{-1} \Leftrightarrow \exists v_i \in k[x]^n : \begin{pmatrix} M_{\beta_1} & M_J & & \\ \vdots & & \cdots & \\ M_{\beta_h} & & & M_J \end{pmatrix} \begin{pmatrix} \lambda \\ v_1 \\ \vdots \\ v_h \end{pmatrix} = 0.$$

Algorithm:

- Compute basis of kernel of big matrix, has rank n and degree $O(d)$.
- Top $n \times n$ matrix yields basis matrix of $J I^{-1}$.

Required time $O(d^2(hn)^3)$.

Ideal basis reduction

Ideal basis reduction for I with $\deg^*(I) = O(g)$:

- Let $d_i = \lceil \deg^*(\omega_i)/n \rceil$. Then $d_i = O(d)$.
- Let M_I be a basis matrix of I with $\deg(M_I) = O(d)$.

Algorithm:

- Multiply the i -th row of M_I by x^{d_i} for all i
- Apply the reduction algorithm.
- Divide the i -th row of the result by x^{d_i} for all i .
- Denote the result by M_I .

The basis elements α_i then satisfy $\deg^*(\alpha_i) \leq \deg^*(I) + 2g$
and there is α_j with $\deg^*(\alpha_j) \leq \deg^*(I) + g$.

Required time $O(d^2n^3)$.

Degree reduction

Degree reduction I with $\deg^*(I) = O(g)$:

- Let M_I be a basis matrix of I with $\deg(M_I) = O(d)$.

Algorithm:

- Apply ideal basis reduction to I , yields new basis matrix M_i .
- Let $z = \alpha_j$ with $\deg^*(\alpha_j) \leq \deg^*(I) + g$.
- Apply simple multiplication and integral division to obtain Rz/I .

The ideal Rz/I satisfies $\deg^*(Rz/I) \leq g$. Apply procedure twice to reduce I .

Required time $O(d^2n^3)$.

Principal ideal test

Principal ideal test for I with $\deg^*(I) = O(g)$:

- $\deg^*(z) \geq \deg^*(I)$ for all $z \in I$,
- $I = Rz$ iff $z \in I$ and $\deg^*(z) = \deg^*(I)$.
- Let α_i be a reduced ideal basis.
- The ideal basis reduction also yields integers $e_1 \leq \dots \leq e_n$ with $\mathcal{L}(I, r) = \{z \in I \mid \deg^*(z) \leq rn\} = \{\sum_i \lambda_i \alpha_i \mid \deg(\lambda_i) \leq -e_i + r\}$ for all $r \in \mathbb{Z}$.
- If $z \in R$ such that $\deg^*(zI) = rn$, then zI principal iff $\mathcal{L}(zI, r) \neq 0$.

Algorithm:

- Compute $z \in R$ such that $\deg^*(zI) = rn$ and $\deg^*(z) = O(g)$.
(Precomputation for all possible degrees of I).
- Using ideal basis reduction on zI check $\mathcal{L}(zI, r) \neq 0$.

Required time $O(d^2n^3)$.

Ideal generating sets

Time for integral division is $O(d^2(hn)^3)$.

Let I be an ideal with $\deg^*(I) = O(g)$ and reduced basis α_i .

Let $h = \max\{\log_q(g), 2\}$.

Proposition (KM):

- A random choice of h elements β_j of $\sum_{i=1}^n k\alpha_i$ is a generating system for I with probability $\geq 1/2$.

Algorithm for integral division:

- Choose h random such β_j (for $n = O(1)$ we can take the α_i).
- Compute reduced basis of $J / \sum_j R\beta_j$.
- If $\deg^*(J / \sum_j R\beta_j) \neq \deg^*(J) - \deg^*(I)$ then repeat.

Required expected time $O^\sim(d^2n^3)$.

Multiplication table speed up

Time for representation matrix computation $O(d^2n^3)$.

Use FFT inspired/based technique:

- Work in $R/Rx^{O(d)}$, can lift elements of small degree back to R .
- Assume there is $y \in R$ such that $\gcd((R : k[x, y]), x) = 1$.
- Then $R/x^d \cong k[x, y]/x^d$, are free $k[x]/x^d$ -modules.
- Isomorphism evaluated by multiplication of unimodular $n \times n$ matrix of degree $\leq d$.
- Multiplication in $k[x, y]/x^d$ in time $O(d^2n^2)$ or $O^\sim(dn)$.

Pairing computation

Need to evaluate the functions $z \in R$ occurring in **simple multiplication** and **principal ideal test**:

- Compute norm of z in R/J over k .
- If zero then choose different equivalent J .
- No inversions necessary.
- Maybe can use J for FFT inspired technique simultaneously (counted before as precomputation).
- $O(\log_2(r))$ evaluations in total.

Runtime not evaluated yet ...

Conclusion

The overall running time for arithmetic in $\text{Pic}^0(F)$ is

$$O^\sim(d^2n^3) = O^\sim(g^2n)$$

where $dn = g$.

- For $d = O(1)$ we obtain $O^\sim(g^3)$ (KM).
- For $n = O(1)$ we obtain $O(g^2)$ (H).
- For $C_{a,b}$ curves we obtain $O^\sim(g^{5/2})$.

The running time linkable to linear algebra over polynomial rings with $nd = g$, should result in $O^\sim(dn^\omega) = O^\sim(gn^{\omega-1})$.

An $n = O(1)$ and time $O(g^2)$ or $O^\sim(g)$ implementation is available in the computer algebra systems Kash and Magma.

Pairings should be similar ... runtime $O^\sim(\log_2(r)gn^{\omega-1})$.