Arithmetic on general curves and applications

ECC Copenhagen, 22.09.2005

Florian Hess
Berlin University of Technology

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:

- Helpful to estimate practicality of index calculus attacks.
- When computing pairings on high genus curves.
- Construction of algebraic geometric codes with good parameters.

Divisor class group

Let $F = k(C)$ be the function field of the irreducible curve C.

Places P of F:

- Surjective valuation $v_P : F \to \mathbb{Z} \cup \{\infty\}$.

Divisors D of F:

- $D = \sum_P n_P P$ with $n_P \in \mathbb{Z}$ almost all zero.
- $v_P(D) := n_P, \ \deg(D) := \sum_P n_P \deg(P)$.
- $(a) := \sum_P v_P(a)P$ for $a \in F^\times$ principal divisor, $\deg((a)) = 0$.

Divisor class group:

- $\mathrm{Cl}^0(F) =$ (group of degree zero divisors)/(group of principal divisors).
- Elliptic curves: $E(k) \cong \mathrm{Cl}^0(k(E)),\ P \mapsto [(P) - (\infty)]$.

Riemann-Roch

Theorem of Riemann-Roch and genus:

- $D_1 \geq D_2 :\Leftrightarrow v_P(D_1) \geq v_P(D_2)$ for all P.
- $\mathcal{L}(D) := \{ a \in F^\times \mid (a) \geq -D \} \cup \{0\}$ is a k-vector space.
- $\dim(\mathcal{L}(D)) = \deg(D) + 1 - g + i(D)$ with $0 \leq i(D) \leq g$.

Riemann-Roch problem:

- Compute $\mathcal{L}(D)$!

Example:

- $F = k(x)$,
- $P_1 = \infty$ with $v_\infty(z) = -\deg(z)$ for $z \in F$,
- $P_2 = (x-1)$ with $v_{(x-1)}(z) =$ power of $x-1$ in z for $z \in F$,
- $D = 7P_1 - 2P_2$.
- Then $\mathcal{L}(D) = \{\sum_{i=0}^{5} \lambda_i x^i (x-1)^2 \mid \lambda_i \in k\}$.

Relation to divisor class groups

Equality of divisor class groups:

- Let $[D], [E] \in \mathrm{Cl}^0(F)$. Then $[E] = [D]$ iff $\mathcal{L}(E - D) \neq 0$.

Unique class representatives:

- Let A be a fixed divisor with $\deg(A) = 1$.
- For $[D] \in \mathrm{Cl}^0(F)$ let $z \in \mathcal{L}(D + rA)$ with $r \geq 0$ minimal. Write $D_0 = D + rA + (z)$.
- Then $D_0 \geq 0$, $\deg(D_0) \leq g$, $[D_0 - rA] = [D]$ and D_0 is uniquely determined.

Tangent-and-chord method for elliptic curves in one step:

- $A = \infty$. $D = (P) - (\infty) + (Q) - (\infty)$.
- Can choose $r = 1$ because $g = 1$.
- $D_0 = (P + Q)$. $(P + Q) - (\infty) = (P) - (\infty) + (Q) - (\infty) + (z)$.

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 $g \to \infty$:

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 $g \to \infty$ (ctd):

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

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 ($n \gtrapprox g/2$).
- 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 $\deg(P) = 1$,
- $R = \mathrm{IntCl}(k[x], F)$.
- $n = O(g)$.

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.
- $\mathrm{Cl}(R) = ($ group of fractional ideals $)/($ group of principal ideals $)$.
- $\mathrm{Cl}(R) \cong \mathrm{Cl}^0(F)$.

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 $J \mid I$.

Degree reduction:

- Rz/I has small degree if $z \in I$ has degree close to that of I.
- Do not neccessarily get unique reduction ...

Arithmetic in the ideal class group

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

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

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

- 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 $\omega_1, \ldots, \omega_n \in R$ of R:

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

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 $M_I \in k[x]^{n \times n}$: $(\alpha_1, \ldots, \alpha_n) = (\omega_1, \ldots, \omega_n) M_I$.

Principal ideal I:

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

Degree function:

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

Bounded representations

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

Theorem:

1. Elements of Cl(R) can be represented by integral ideals I with $\deg^*(I) = O(g)$.
2. $\deg^*(I) = O(g)$ iff there is a basis matrix M_I with $\deg(M_I) = O(d)$.
3. $\deg^*(\sum_i \lambda_i \omega_i) = O(g)$ iff $\deg(\lambda_i) = O(d)$ for all i.
4. There is a basis α_i of I with $\deg^*(\alpha_i) = \deg^*(I) + O(g)$ for all i.

Represent elements of Cl(R) by integral ideals with $n \times n$ basis matrices of degree $O(d)$.

(KM proceeds in the end quite similar ...)

Linear algebra over polynomial rings

References: Storjohann, Villard, ...

Matrix multiplication in dimension n and degree d:

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

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

- Let $M = (v_1, \ldots, v_m) \in k[x]^{n \times m}$, 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 $O(d^2 nmr)$.

Kernel of M:

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

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 $\deg^*(\alpha_i) \le \deg^*(I) + O(g)$.
Hence $\deg(M_I) \le cd$ for some absolute constant c.

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

Simple multiplication

Compute reduced basis of 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 $z\omega_j = \sum_\nu (\sum_i \mu_i \lambda_{i,j,\nu})\omega_\nu$.
- Multiply M_z and basis matrix of I to obtain a basis matrix of zI.
- Apply ideal basis reduction.

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

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

Integral division

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

- 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 $\lambda = (\lambda_1, \ldots, \lambda_n)^t \in k[x]^n$:

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

Algorithm:

- Compute basis of kernel of big matrix, has rank n and degree $O(d)$.
- Apply ideal basis reduction to top $n \times n$ matrix.

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

(For h big compute kernel in a different way.)

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 $e_1 \leq \cdots \leq e_n$ 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 $\deg^*(z) = O(g)$.
- Using ideal basis reduction on zI check $\mathcal{L}(zI, r) \neq 0$.

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

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

Multiplication table speed up

Time for representation matrix computation $O(d^2n^3)$.
Use FFT inspired technique:

Define $\phi : \mathcal{L}(2r \cdot P) \to \prod_j R/\mathfrak{p}_j^{r_j}$ with $\sum_j r_j \deg^*(\mathfrak{p}_j) > 2r$
for some large enough $r = O(g)$.

ϕ is injective, k-linear and $\phi(z_1z_2) = \phi(z_1)\phi(z_2)$ for $z_1, z_2 \in \mathcal{L}(r \cdot P)$.

KM: For $d = O(1)$ we only have to do linear algebra over k.

- Hence do all computations in $\prod_j R/\mathfrak{p}_j^{r_j}$.
- Choose for example $r_j = 1$ and $\deg(\mathfrak{p}_j) = 1$.
- Then representation matrix computation requires time $O(g^2)$.

Multiplication table speed up

Assume there is $y \in R$ with $\omega_i = y^{i-1}$.

- Then $(n-1)(\deg^*(y) - 1) = 2g$ and we have a $C_{a,b}$ curve.
- Plane curve equation has degree n in y and degree $O(d)$ in x.
- Representation matrix computation requires time $O(d^2n^2)$.

Faster linear algebra over polynomials:

- the required operations should have running time $O^\sim(dn^\omega)$.
- Representation matrix computation should be possible
  in time $O^\sim(dn^\omega)$ using the FFT inspired technique and completions.

Conclusion

The overall running time 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 should be completely linkable to linear
algebra over polynomial rings, resulting in $O^\sim(dn^\omega) = O^\sim(gn^{\omega-1})$.

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