Computation of Riemann-Roch Spaces and Some Applications

Sage Days
May 26th, 2010

Florian Hess
Otto-von-Guericke-Universität Magdeburg

Curves and function fields

Let

- k be an arbitrary perfect base field (later $k = \mathbb{F}_q$).
- C_0 an irreducible algebraic curve over k.
- $F = k(C_0)$ function field of C_0.
- C irreducible complete regular curve over k defined by F/k.

Example:

- $C_0 : y^2 = x^7 - 1$ over $k = \mathbb{Q}$.
- $C : y^2 = zx^7 - z^8$ where $w(x) = w(z) = 1$ and $w(y) = 4$.

C_0 and C need not be absolutely irreducible, or k need not be algebraically closed in F.

Points and places

Places = maximal ideals of discrete valuation rings in F/k
= scheme theoretic points of C.

A place P defines

- local ring $\mathfrak{o}_P$,
- residue class field $k(P) = \mathfrak{o}_P/P$, $\deg(P) := [k(P) : k]$,
- evaluation map $F \to k(P) \cup \{\infty\}$, $a \mapsto a \bmod P$,
- valuation $v_P : F \to \mathbb{Z} \cup \{\infty\}$.

Example:

- $F = k(x)$,
- $P_1 = (x-1)$ with $v_{(x-1)}(z)$ = power of $x-1$ in z for $z \in F$,
- $P_2 = \infty$ with $v_\infty(z) = -\deg(z)$ for $z \in F$.

Divisors

Divisors = finite formal sum of places with integral multiples
$D = \sum_P n_P P$ mit $n_P \in \mathbb{Z}$ almost all zero.

Principal divisor $D = \mathrm{div}(f) := \sum_P v_P(f)P$ für $f \in F^\times$.

Example:

- $D = 7P_2 - 2P_1$.
- $\mathrm{div}(x-1) = P_1 - P_2$

Degrees:

- $\deg(D) = \sum_P n_P \deg(P)$. $\deg(f) := \deg(\sum_{n_P>0} n_P \deg(P))$.
- Have $\deg(f) = [F : k(f)]$ and $\deg(\mathrm{div}(f)) = 0$.

$v_P(D) := n_P$.
$D_1 \geq D_2 :\Leftrightarrow v_P(D_1) \geq v_P(D_2)$ for all P.
$\mathrm{supp}(D) := \{P \mid v_P(D) \neq 0\}$.

Riemann-Roch

$\mathcal{L}(D) := \{\, a \in F^\times \mid \mathrm{div}(a) \geq -D \,\} \cup \{0\}$ is a k-vector space.

Theorem: There is a divisor W and $g \geq 0$ such that for all divisors D:

$$\dim(\mathcal{L}(D)) = \deg(D) + 1 - g + \dim(\mathcal{L}(W - D)).$$

Here W canonical divisor, g genus of F/k and C.

Example:

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

Constructive Riemann-Roch

Input is C_0 and algorithms for k, $k[x]$ and $k[x]^{n \times n}$.

Tasks: Represent functions, places and divisors. Compute with

- residue class fields $k(P)$, valuations v_P.
- k-linear algebra in F.
- bases of Riemann Roch spaces $\mathcal{L}(D)$.
- Canonical divisors W, genus g, exact constant field $\mathcal{L}(0)$.

Complexity measures:

- Count operations in k and $\mathbb{Z}$ depending on input length in k and $\mathbb{Z}$.
- Main dependency on C_0, g, $\deg(P)$, $\mathrm{ht}(D) := \sum_P |v_P(D)| \deg(P)$.
- Want (best) polynomial time.

Picard groups

$\mathrm{Div}(C)$ divisor group, $\mathrm{Div}^0(C)$ subgroup of divisors of degree 0.
$\mathrm{Prin}(C)$ group of principal divisors.

$\mathrm{Pic}(C) = \mathrm{Div}(C)/\mathrm{Prin}(C)$ Picard group.
$\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{Prin}(C)$ degree zero Picard group.

Have

- $\mathrm{Pic}(C) \cong \mathbb{Z} \oplus \mathrm{Pic}^0(C)$.
- $\mathrm{Pic}^0(C) \cong$ Jac$(C)(k)$.

Example:

- $\mathrm{Pic}^0(\mathbb{P}^1) = 1$
- $\mathrm{Pic}^0(E) \cong E(k)$.

Riemann Roch and Picard groups

Equality of divisor classes:

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

Unique class representatives:

- Let A be a place of degree one.
- For $[D] \in \mathrm{Pic}^0(C)$ let $z \in \mathcal{L}(D + rA)$ with $r \geq 0$ minimal. Write $\tilde{D} = D + rA + (z)$.
- Then $\tilde{D} \geq 0$, $\deg(\tilde{D}) \leq g$, $[\tilde{D} - rA] = [D]$ and $\tilde{D}$ 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 $g = 1$.
- $\tilde{D} = (P + Q)$. $(P + Q) - (\infty) = (P) - (\infty) + (Q) - (\infty) + (z)$.

Pairings

Evaluation of functions at divisors:

- $f \in F^\times$, $D \in \mathrm{Div}(C)$.
- $f(D) := \prod_P N_{k(P)/k}(f \bmod P)^{v_P(D)}$.

Only defined when $v_P(f) = 0$ for $P \in \mathrm{supp}(D)$.

Approximation Theorem:

- Let $D, E \in \mathrm{Div}(C)$.
- There is $h \in F^\times$ such that $\mathrm{supp}(D + \mathrm{div}(h)) \cap \mathrm{supp}(E) = \emptyset$.

Weil reciprocity:

- $f(\mathrm{div}(h)) = h(\mathrm{div}(f))$.

Pairings

Let $r \geq 1$, $\gcd(r, \mathrm{char}(k)) = 1$ and assume $\mu_r \subseteq k$.

Weil pairing:

$$e_r : \mathrm{Pic}^0(C)[r] \times \mathrm{Pic}^0(C)[r] \to \mu_r$$

- $[D], [E] \in \mathrm{Pic}^0(C)[r]$, $\mathrm{div}(f) = rD$, $\mathrm{div}(h) = rE$.
- $e_r([D],[E]) = h(D)/f(E)$.
- bilinear, antisymmetric, non degenerate if $\#\mathrm{Pic}^0(C)[r] = r^{2g}$.

Tate-Lichtenbaum pairing for $k = \mathbb{F}_q$:

$$t_r : \mathrm{Pic}^0(C)[r] \times \mathrm{Pic}^0(C)/r\mathrm{Pic}^0(C) \to \mu_r$$

- $[D] \in \mathrm{Pic}^0(C)[r]$, $[E] \in \mathrm{Pic}^0(C)$, $\mathrm{div}(f) = rD$.
- $t_r([D],[E]) = f(E)^{(q^k-1)/r}$.
- bilinear, non-degenerate.

Remarks

The Weil and Tate-Lichtenbaum pairings have geometric generalisations to abelian varieties ⇒ arithmetic duality.

Here specialisation to Jacobians ⇒ class field theory.
Useful: Description in terms of 1-dimensional objects possible.

Properties of pairings:

- Well-definedness and bilinearity easy with Weil reciprocity.
- Non-degeneracy via arithmetic duality / class field theory.

Riemann Roch and pairings

Need to compute:

- $\mathrm{div}(f) = rD \Leftrightarrow f \in \mathcal{L}(-rD)$.
- $f(E) = \prod_P N_{k(P)/k}(f \bmod P)^{v_P(E)}$.

Can assume: $\mathrm{ht}(D), \mathrm{ht}(E) = O(g)$.

Problem: Well possible that $r \approx q^g$, so $\mathrm{ht}(-rD)$ exponential in g.

Using divisor reduction:

- Can write $f = \prod_{i=0}^{\log_2(r)} f_i^{2^i}$ with $\deg(f) = O(g)$.
- Yields a generalised Miller algorithm.
- Runtime essentially $\log_2(r)$ evaluations $f_i(E)$.

Riemann Roch and pairings

Need to have $\mathrm{supp}(D) \cap \mathrm{supp}(E) = \emptyset$.

Translation and divisor reduction:

- Choose a place A with $\deg(A) = 1$ and $A \notin \mathrm{supp}(D)$.
- Write $D = \tilde{D} - rA - (z)$ as before.
- If $\mathrm{supp}(\tilde{D}) \cap \mathrm{supp}(E) = \emptyset$, use $\tilde{D} - rA$ instead of D.

Example:

- $D = (P) - (\infty)$, $A = Q$, $r = 1$,
- $\tilde{D} = (P + Q)$,
- $\tilde{D} - rA = (P + Q) - (P)$.

Riemann Roch and pairings

Need to have $\mathrm{supp}(D) \cap \mathrm{supp}(E) = \emptyset$.

Approximation theorem:

- Choose a place A with $\deg(A) = 1$ and $A \notin \mathrm{supp}(E)$.
- Define $E_P = \sum_{Q \in \mathrm{supp}(E) \setminus \{P\}} Q$ for $P \in \mathrm{supp}(E)$.
- Choose r sufficiently large such that there is $z_P \in \mathcal{L}(D + rA - E_P) \setminus \mathcal{L}(D + rA - E_P - P)$ for all $P \in \mathrm{supp}(E)$.
- $\Rightarrow$ $v_P(z_P) = v_P(-D)$ and $v_Q(z_P) > v_Q(-D)$ for all $Q \in \mathrm{supp}(E) \setminus \{P\}$.
- $\Rightarrow$ $z := \sum_P z_P$ satisfies $v_P(z) = v_P(-D)$ for all $P \in \mathrm{supp}(E)$.
- $\Rightarrow$ $\mathrm{supp}(D + \mathrm{div}(z)) \cap \mathrm{supp}(E) = \emptyset$.

Basic algorithms

Representation of F and C:

- Using C_0 we find a complete C_1 birational to C_0 with a finite separable surjective morphism $C_1 \to \mathbb{P}^1$ of degree n.
- $F = k(x)[y]$ with $f(y) = 0$ for $f \in k(x)[t]$.
- $E = F[z]$ with $h(z) = 0$ for $h \in F[t]$.
- C_1 represented by some R_i-orders O_i with $R_i \subseteq k(x)$.
- C represented by integral closures $\mathrm{Cl}(R_i, F)$.
- $\mathbb{P}^1 = \cup_i \mathrm{Spec}(R_i)$, $C_1 = \cup_i \mathrm{Spec}(O_i)$, $C = \cup_i \mathrm{Spec}(\mathrm{Cl}(R_i, F))$.
- R_i principal ideal domain, e.g. $R_i = k[x], R_j = k[1/x]$.

O_i and $\mathrm{Cl}(R_i, F)$ have bases of the form $\omega_1, \ldots, \omega_n$ and there are $\lambda_{i,j,\nu} \in R_i$ with $\omega_i \omega_j = \sum_{\nu=1}^{n} \lambda_{i,j,\nu} \omega_\nu$.

Bases of $\mathrm{Cl}(R_i, F)$ lead to regular affine curves.

Basic algorithms

Algorithmic number theory (over $\mathbb{Z}$) provides essentially everything that is needed in O_i and $\mathrm{Cl}(R_i, F)$:

- integral closures,
- ideal arithmetic and factoring,
- valuations, residue class fields,
- differents and discriminants.

Much is reduced to linear algebra over R_i, avoids potentially expensive Gröbner basis computations (have n variables).

Places and divisors

$$\mathfrak{o}_\infty := \{\, g/h \mid g,h \in k[x] \text{ and } \deg(g) \le \deg(h) \,\},$$

$$\begin{tikzcd}
F \arrow[d, dash, "n"] & \mathrm{Cl}(k[x],F) \arrow[d, dash, "n"] & \mathrm{Cl}(\mathfrak{o}_\infty,F) \arrow[d, dash, "n"] \\
k(x) & k[x] & \mathfrak{o}_\infty \\
P_1 \arrow[r, dashed, leftrightarrow] & \mathfrak{p}_1 & \\
P_2 \arrow[rr, dashed, leftrightarrow] & & \mathfrak{p}_2 \\
D \arrow[r, dashed, leftrightarrow, bend right] \arrow[rr, dashed, leftrightarrow, bend left] & \mathfrak{d}_1 & \mathfrak{d}_2
\end{tikzcd}$$

$$\mathcal{L}(D) \quad = \quad \mathfrak{d}_1^{-1} \quad \cap \quad \mathfrak{d}_2^{-1}$$

Intersection

$k[x]$-basis of $\mathfrak{d}_1^{-1}$: $a_1,\ldots,a_n$, $\mathfrak{o}_\infty$-basis of $\mathfrak{d}_2^{-1}$: $b_1,\ldots,b_n$.
$M \in k(x)^{n\times n}$: $(b_1,\ldots,b_n)M = (a_1,\ldots,a_n)$

Lemma (“LLL” algorithm):
$\exists\, R \in \mathrm{GL}_n(\mathfrak{o}_\infty)$, $T \in \mathrm{GL}_n(k[x])$, $d_i \in \mathbb{Z}$: $RMT = \left(x^{-d_i}\delta_{i,j}\right)_{i,j}$.

Suppose $M = \left(x^{-d_i}\delta_{i,j}\right)_{i,j}$ and $c = \sum_{i=1}^n \lambda_i a_i$:
Then $c \in \mathcal{L}(D) \Leftrightarrow \lambda_i \in k[x]$ and $x^{-d_i}\lambda_i \in \mathfrak{o}_\infty$.

Let $B_r := \{\, x^j a_i \mid 1 \le i \le n,\, 0 \le j \le d_i + r \,\}$.

Theorem: B_r is k-basis of $\mathcal{L}\big(D + r(x)_\infty\big)$ for all $r \in \mathbb{Z}$

Can replace $\mathfrak{o}_\infty$ by $k[1/x]$ in all statements.

Divisor reduction

Problem: Compute $\mathcal{L}(D)$ if D has large exponents or large degree.

Let A be a divisor with $\deg(A) \ge 1$ and g the genus of F/k.
For D there is $\tilde{D} \ge 0$ with $D = \tilde{D} - rA - (z)$ and $\deg(\tilde{D}) \le g + \deg(A) - 1$.
$\tilde{D}$ is uniquely determined, if r minimal and A place with $\deg(A) = 1$.

- Choose $z \in \mathcal{L}(D + rA)$ and let $\tilde{D} = D + rA + (z)$.
- Given $D_3 = D_1 + D_2$, $\tilde{D}_3$ is easily computed from $\tilde{D}_1 + \tilde{D}_2$ alone.

Yields „double-and-add“ method ...

Divisor reduction

„Double-and-add“ method with divisor reduction:

- Write $D = \sum_{i=0}^m 2^i D_i$ with all exponents in D_i one.
- Evaluate horner-like $D = 2(\cdots(2D_1 + D_0)\cdots)$, and apply divisor reduction to intermediate results.
- Leads to $\tilde{D} = D + rA + (z)$ with $z = \prod_{i=0}^{\log_2(r)} z_i^{2^i}$.
- If D_i large than apply divisor reduction successively also to D_i as a precomputation.
- Leads to $\tilde{D} = D + rA + (z)$ with $z = \prod_{i=0}^{\log_2(r)} (z_i \prod_{j=1}^{t_i} z_{i,j})^{2^i}$.
- $\deg(z_i) = O(g)$, $\deg(z_{i,j}) = O(g)$ if $\max\{\deg(P) \mid P \in \mathrm{supp}(D_i)\} = O(g)$.
  $t_i = O(\#\mathrm{supp}(D_i))$.

Thus log-dependency on expos and linear dependence on $\#\mathrm{supp}(D)$.
Resulting objects of degree $O(g)$ if $\max\{\deg(P) \mid P \in \mathrm{supp}(D)\} = O(g)$.

Divisor reduction

Computation of $\mathcal{L}(D)$ for large D:

- Apply divisor reduction $\tilde{D} = D + rA + (z)$.
- Compute $\mathcal{L}(\tilde{D} - rA)$.
- Have $\mathcal{L}(D) \cong \mathcal{L}(\tilde{D} - rA)$ under $f \mapsto f/z$.

If $\deg(D)$ large then use $A = (x)_\infty$:

- parametric bases B_r also for large r efficient.

Summary: Computation of $\mathcal{L}(D)$ works efficient in n, g if $\max\{\deg(P) \,|\, P \in \mathrm{supp}(D)\} = O(g)$ and $\#\mathrm{supp}(D) = O(g)$.

Representation of divisors

Useful data types for / representation of divisors:

- Free representation as sum of places with multiplicities.
- Ideal representation in terms of (inverses) of ideals on affine patches.
- Reduced representation via $D = \tilde{D} + rA + (z)$.

Useful data types for / representation of algebraic function:

- Product representation with multiplicative support (evaluation, norms, principal divisor, factorisation, equality).
- ...

Computing in Picard groups

In $\mathrm{Pic}(C)$:

- Principal divisor test, divisor reduction, with $\deg(A) = 1$ unique class representatives.

In $\mathrm{Pic}(\mathrm{Cl}(k[x], F))$:

- Let $S = \mathrm{Spec}(\mathrm{Cl}(\mathfrak{o}_\infty, F))$.
- Have $\mathrm{Pic}(\mathrm{Cl}(k[x], F)) \cong \mathrm{Pic}(C)/\langle S \rangle$.
- Need to test membership $[D] \in \langle S \rangle$.
- Easy for $\#S = 1$, otherwise solve DLP. Better use pairings?

After a precomputation complexity for one group operation in $\mathrm{Pic}^0(C)$ between $O(g^2)$ and $O(g^4)$.

Applications

Algebraic-geometric codes $\{(f(P_1), \ldots, f(P_n)) \,|\, f \in \mathcal{L}(D)\}$.

Differentials: $\omega = f dx$, $f, x \in F$, x separating element.

Exact constant field: $\mathcal{L}(0)$.

Gap numbers and Weierstrass places.

Structure of Picard groups of curves over finite fields, DLP.

Tate pairing on Picard groups (multiplicative and additive version).

Class fields, curves with many rational points, good codes.

Isomorphisms and automorphisms of function fields.

...