

Computing Zeta Functions of Non-degenerate Curves

W. Castryck, J. Denef and F. Vercauteren

Katholieke Universiteit Leuven

31 May 2005

Non-degenerate Curves

Lifting Frobenius

Reduction Algorithm

Non-degenerate Curves (1)

- ▶ Let $q = p^n$ with p prime and let k be either \mathbb{F}_q or \mathbb{Q}_q
- ▶ Let C be the affine curve $f(x, y) = 0$ with $f(x, y) \in k[x, y]$
- ▶ Write $f(x, y) = \sum_{(i,j) \in S} f_{i,j} x^i y^j$ with $f_{i,j} \neq 0$ and $S \subset \mathbb{Z}^2$
- ▶ S is called the *support* of f , convex hull of S is the *Newton polygon* $\Gamma(f)$ of f

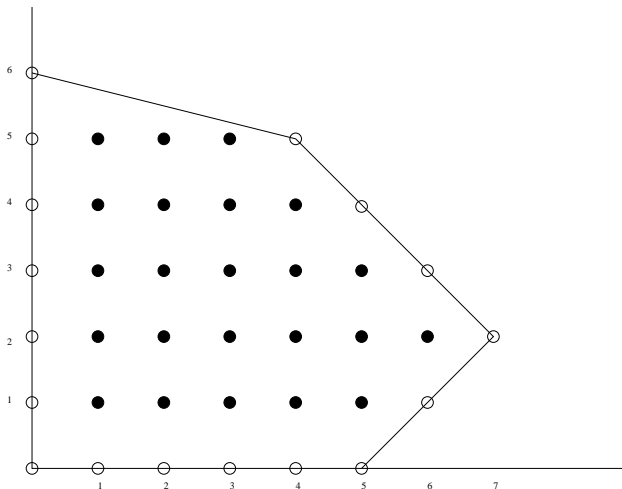
Definition

$f(x, y)$ is called *non-degenerate* w.r.t. its Newton polygon Γ if for all faces σ of Γ (including Γ) and $f_\sigma = \sum_{(i,j) \in \sigma} f_{i,j} x^i y^j$

$$f_\sigma, \quad \frac{\partial f_\sigma}{\partial x} \quad \text{and} \quad \frac{\partial f_\sigma}{\partial y}$$

have no common zero in $\mathbb{T} = (\mathbb{A} \setminus \{0\})^2$ over \bar{k}

Non-degenerate Curves (2)



Toric Varieties

- ▶ Let Co be a cone in \mathbb{R}^2
- ▶ $k[Co]$ is k -algebra generated by $x^i y^j$ with $(i, j) \in Co$
- ▶ Denote by X_{Co} the affine toric k -variety $\text{Spec}(k[Co])$

Example

- ▶ Let $Co = \langle (1, 0), (0, 1) \rangle$, then $X_{Co} = \mathbb{A}^2$
- ▶ Let $Co = \langle (1, 0), (-1, 0), (0, 1) \rangle$, then

$$k[Co] = k[x, y, x^{-1}] \quad \text{and} \quad X_{Co} \simeq \mathbb{A}^1 \times (\mathbb{A}^1 \setminus \{0\})$$

- ▶ Let $Co = \langle (1, 0), (0, 1), (-1, 0), (0, -1) \rangle$, then

$$k[Co] = k[x, y, x^{-1}, y^{-1}] \quad \text{and} \quad X_{Co} = \text{Spec}(k[Co]) = \mathbb{T}$$

Toric Resolution

- ▶ Construct toric compactification X_Γ of \mathbb{T} associated with Newton polyogon Γ
- ▶ Let σ be an edge of Γ and let $Co_\sigma = \langle x - p \mid x \in \Gamma, p \in \sigma \rangle$ be a half-plane
- ▶ Define U_σ to be the toric variety $X_{Co_\sigma} \simeq \mathbb{A}^1 \times (\mathbb{A}^1 \setminus \{0\})$
- ▶ X_Γ is covered by U_σ for σ an edge of Γ
- ▶ U_{σ_1} and U_{σ_2} glued together along \mathbb{T}

Lemma

$X_\Gamma \setminus \mathbb{T} = \cup_{i=1, \dots, r} L_i$ with $L_i = X_{\text{Lin}(\sigma_i)} \simeq \mathbb{A}^1$ and $\text{Lin}(\sigma_i) = \langle v_i \rangle$
 with v_i vector parallel to edge σ_i

Toric Resolution

- ▶ Let \mathcal{C} be the closure of $\{(x, y) \in \mathbb{T} \mid f(x, y) = 0\}$ in X_Γ
- ▶ \mathcal{C} is complete, non-singular curve
- ▶ Genus of \mathcal{C} is number of integral points in interior of Γ
- ▶ \mathcal{C} intersects each L_i transversally for $i = 1, \dots, r$
- ▶ $|L_i \cap \mathcal{C}| = (\# \text{ lattice points on } \sigma_i) - 1$
- ▶ Let e_i be vector with integral coefficients and $\perp \sigma_i$, then

$$\text{Div}_{\mathcal{C}}(x^i y^j) = \sum_{k=1, \dots, r} (i, j) \cdot e_k (L_k \cap \mathcal{C})$$

Lifting Curve

- ▶ Let $\bar{C} : \bar{f}(x, y) = 0$ with $\bar{f} \in \mathbb{F}_q[x, y]$ and assume that \bar{f} is non-degenerate w.r.t. $\Gamma(\bar{f})$
- ▶ Assume that \bar{f} is *monic in y* of degree d and *commode*
- ▶ Take *arbitrary lift* $f(x, y) \in \mathbb{Z}_q[x, y]$ with $\Gamma(\bar{f}) = \Gamma(f)$
- ▶ $f(x, y)$ is again non-degenerate w.r.t. the Newton polygon Γ
- ▶ Genus $g(\bar{C}) = g(C)$ and one-to-one correspondence between points at infinity
- ▶ Let A^\dagger be the dagger ring of $A := \mathbb{Z}_q[x, y]/(C)$.
- ▶ Elements of A^\dagger can be represented as

$$\sum_{l=0}^{d-1} \sum_{k=0}^{+\infty} a_{k,l} x^k y^l$$

and the valuation of $a_{k,l} \in \mathbb{Z}_q$ grows linearly with k

A Lift of the Frobenius Endomorphism

- ▶ The necessary conditions on the Frobenius Σ on A^\dagger are

$$\Sigma(x) \equiv x^p \pmod{p} \quad \Sigma(y) \equiv y^p \pmod{p} \quad C^\Sigma(\Sigma(x), \Sigma(y)) = 0$$

- ▶ Main idea: lift Frobenius on x and y simultaneously such that denominator in the Newton iteration is invertible in A^\dagger
- ▶ Let $Z \in A^\dagger$ such that $\Sigma(x) = x^p + \alpha Z$ and $\Sigma(y) = y^p + \beta Z$,

$$C^\Sigma(\Sigma(x), \Sigma(y)) = C^\Sigma(x^p + \alpha Z, y^p + \beta Z) = 0$$

and

$$Z \equiv 0 \pmod{p}$$

A Lift of the Frobenius Endomorphism

- ▶ Let $G(Z) := C^\Sigma(x^p + \alpha Z, y^p + \beta Z)$, then

$$G'(Z) \equiv \alpha \frac{\partial C^\Sigma}{\partial x} \Big|_{(x^p, y^p)} + \beta \frac{\partial C^\Sigma}{\partial y} \Big|_{(x^p, y^p)} + O(Z) \pmod{p}$$

- ▶ $G'(Z)$ will be invertible in A^\dagger if $G'(Z) \equiv 1 \pmod{p}$ and thus

$$G'(Z) \equiv \alpha \left(\frac{\partial C}{\partial x} \right)^p + \beta \left(\frac{\partial C}{\partial y} \right)^p \equiv 1 \pmod{p}$$

- ▶ Since \bar{C} non-singular, $\frac{\partial \bar{C}}{\partial x}$, $\frac{\partial \bar{C}}{\partial y}$ and \bar{C} generate unit ideal and using Buchberger's algorithm we compute $\bar{\alpha}, \bar{\beta}, \bar{\gamma} \in \bar{A}$ with

$$1 = \bar{\alpha} \left(\frac{\partial \bar{C}}{\partial x} \right)^p + \bar{\beta} \left(\frac{\partial \bar{C}}{\partial y} \right)^p + \bar{\gamma} \bar{C}$$

A Lift of the Frobenius Endomorphism

- ▶ Convergence rate of $Z = \sum_{l=0}^{d-1} \sum_{k=0}^{+\infty} a_{k,l} x^k y^l$ is given by

$$\text{ord}_p a_{i,j} \geq \frac{i + (d_C - d + 1)j}{6p(d + 1)(d_C - d + 1)}$$

with d_C the total degree of C

- ▶ Proof requires *linear effective Nullstellensatz*: let $f_0, f_1, f_2 \in k[x, y]$ with support in Γ and f_0, f_1, f_2 have no common solution in X_Γ , then $\exists h_0, h_1, h_2$ with support in 2Γ

$$1 = h_0 f_0 + h_1 f_1 + h_2 f_2$$

Two Divisors and Riemann-Roch

Definition

Let D_C be the divisor on \mathcal{C}

$$D_C := - \sum_{i=1, \dots, r} N_i(L_i \cap \mathcal{C}), \quad \text{with } N_i = p_i \cdot e_i$$

with p_i any vertex on edge σ_i and let $W_C := \sum_{i=1, \dots, r} (L_i \cap \mathcal{C})$

Theorem

The Riemann-Roch space

$$\mathcal{L}(mD_C) = \{h \in k(\mathcal{C}) \mid \text{Div}(h) \geq -mD_C\}$$

is generated by $x^i y^j$ with $(i, j) \in m\Gamma$

From differentials to polynomials ...

- ▶ Consider the map $\Lambda : k(C) \rightarrow \Omega(C) :$

$$h(x, y) \mapsto \Lambda(h) = h(x, y) \frac{dx}{xyf_y}$$

with $f_y = \partial f / \partial y$

- ▶ An exact differential $\omega = dg$ is the image of

$$dg = g_x dx + g_y dy = (f_y g_x - f_x g_y) \frac{dx}{f_y} = xy \left(f_y \frac{\partial}{\partial x} - f_x \frac{\partial}{\partial y} \right) (g) \frac{dx}{xyf_y}$$

- ▶ Define D operator as

$$D(g) = xy \left(f_y \frac{\partial}{\partial x} - f_x \frac{\partial}{\partial y} \right) (g)$$

then $dg = \Lambda(D(g))$

The Reduction Algorithm

- ▶ Every $\omega \in H_{DR}^1(C)$ can be written as $\Lambda(h)$ with $h \in \mathbb{Q}_q[x, y]$
- ▶ Computing modulo exact differential forms then is equivalent to computing modulo D
- ▶ For subset $E \subset \mathbb{R}^2$ define L_E \mathbb{Q}_q -vectorspace of all Laurent polynomials with support contained in E
- ▶ Let $S_m := \langle x^i y^j \mid 0 \leq i \leq m, 0 \leq j < d \rangle \subset \mathbb{Q}_q[x, y]$
- ▶ Define $\kappa \in \mathbb{N}_0$ smallest integer such that $L_{2\Gamma} \bmod f \subset S_\kappa$

The Reduction Algorithm

Theorem

For all $m \in \mathbb{N}_0$, we have

$$S_m^{(1)} \subset D(S_{m-1+\kappa}^{(0)}) + \mathcal{L}^{(1)}(2D_C)$$

where for a set of polynomials $L \subset \mathbb{Q}_q[x, y]$ we define

$$L^{(0)} = L \cap \mathbb{Z}_q[x, y]$$

$$L^{(1)} = \{h \in L^{(0)} \mid \forall P \in \mathcal{C} \setminus \mathbb{A}^2, \forall i < 0 : i \mid_{\mathbb{Z}_q} \text{Coeff}\left(\frac{t}{dt} \Lambda(h), i\right)\}$$

with t such that (p, t) generates local ring at P of \mathcal{C} over \mathbb{Z}_q

The Reduction Algorithm

- ▶ Given $h(x, y) \in \mathcal{S}_M$ for some $M \in \mathbb{N}_0$
- ▶ Let $\Delta = \max\{-\text{ord}_{P_i}(x^M y^{(d-1)})\}_i$ for all places P_i at ∞
- ▶ Set $\epsilon = \lceil \log_p(\Delta) \rceil$, then $p^\epsilon h(x, y) \in \mathcal{S}_M^{(1)}$
- ▶ Compute $g \in D(\mathcal{S}_{M-1+\kappa}^{(0)})$ such that $h - d(g) \in \mathcal{L}^{(1)}(2D_C)$
- ▶ Choose as basis for $H_{DR}^1(C)$ a \mathbb{Z}_q -module basis of

$$\mathcal{L}^{(0)}(2D_C) / (D(\mathcal{L}(D_C)) \cap \mathbb{Z}_q[x, y])$$

Future Work ...

- ▶ Algorithm also works for non-monic and non-commode polynomials, really computes on torus
- ▶ Make precise complexity estimate, currently think $O(g^6 n^3)$, but could be $O(g^5 n^3)$
- ▶ Does algorithm generalise to higher dimensions?
- ▶ Abandon current lift of Frobenius and try $\Sigma(x) = x^p$ again
- ▶ Why require isomorphism of $H_{DR}^1(C)$ and $H_{MW}^1(\overline{C})$?