Frobenius lifts and point counting for smooth curves

Amnon Besser, Francois Escriva

(Joint with Rob de Jeu) 25/9/2013

Goal

- A new method for point counting on smooth curves.
- Based, like Kedlaya's algorithm, on Monsky-Washnitzer cohomology.
- Timing is comparable (theoretically) with Kedlaya's algorithm.
- arxiv.org/abs/1306.5102

Key new ideas

- Replacing reduction in cohomology by cup product computations.
- A general lift of Frobenius based on Arabia's work.
- Local computation of the lift of Frobenius.

Computing the action of Frobenius on cohomology using cup products

Serre's formula for the cup product

- C/K a smooth complete curve
- $\omega, \eta \in \Omega^1$ of the second kind

Theorem (Serre)

The cup product $\omega \cup \eta \in K$ is given as follows:

$$\omega \cup \eta = \sum_x \operatorname{Res}_x \eta \int \omega \,,$$

where the sum is over all points x and the integral is a local integral with arbitrary constant term.

p-adic cup product formula

K - p-adic

$U = C - \cup D_i$, where D_i are discs

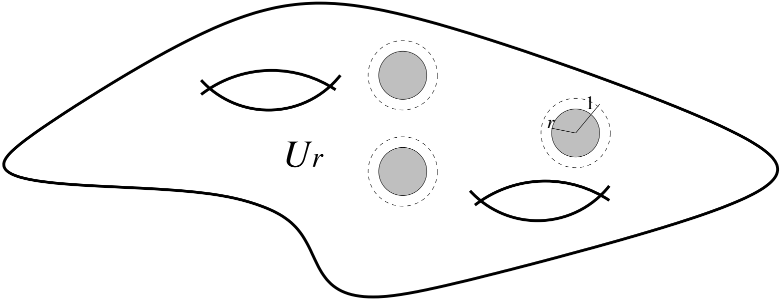

Figure: A wide open space

For $\omega \in \Omega^1(U)$

- Notion of $\mathrm{Res}_{D_i} \omega$
- Notion of "of second kind"
- "cup product like" pairing

$$\langle \omega, \eta \rangle = \sum_i \mathrm{Res}_{D_i} \eta \int \omega$$

Basic observation: $\omega \cup \eta = \langle \omega|_U, \eta|_U \rangle$

Cup product and Frobenius

For U as above we can find (compute) a lift of Frobenius ϕ.
Example: hyperelliptic curve - $U = C -$ Weierstrass discs, $\phi(x, y) = (x^p, \cdots)$.
Restriction $H^1(C) \to H^1(U)$ is compatible with Frobenius.

Corollary

$\omega \cup \phi\eta = \langle \omega \cup \phi\eta \rangle$

Application for computing the matrix of Frobenius

$\{\omega_1, \ldots \omega_{2g}\}$ - a basis for $H^1(C)$

1. Compute M_1 with entries $\omega_i \cup \omega_j$
2. Compute M_2 with entries $\omega_i \cup \phi\omega_j$
3. Matrix of Frobenius is given by $M_1^{-1} M_2$.

Lifting of Frobenius

- The problem with Frobenius lifting is that it is not unique.
- Solution: Impose additional conditions.

Example: 1 equation, 2 variables

$f(x,y)$ in $\mathbb{Z}_p[x,y]$
reduction $\overline{f}(x,y)$ non-singular

$$\overline{P}_1\overline{f}_x + \overline{P}_2\overline{f}_y = 1 + \overline{\Delta}\,\overline{f}\,.$$

Lift $\overline{P}_1$, $\overline{P}_2$ and $\overline{\Delta}$ to P_1, P_2 and Δ in $\mathbb{Z}_p[x,y]$
Then,

$$\phi(x,y) = (x^p, y^p) + s \times (P_1(x^p,y^p), P_2(x^p,y^p))$$

where s in $p\mathbb{Z}_p\langle x,y\rangle$ solves

$$f[(x^p,y^p) + S \times (P_1(x^p,y^p), P_2(x^p,y^p))] \\ - f(x,y)^p - f(x,y)^p\Delta(x^p,y^p)S = 0\,.$$

is a lift of Frobenius.

The equation can be solved since its derivative with respect to S at $S = 0$ is

$$f_x(x^p, y^p)P_1(x^p, y^p) + f_y(x^p, y^p)P_2(x^p, y^p) - f(x^p, y^p)\Delta(x^p, y^p),$$

which is 1 modulo p.
s is found using Newton iterations.
It is **unique** once P_1, P_2 and Δ are chosen.

Local liftings of Frobenius

For a disc D with parameter t we need the expansion $\phi(t)$.

- Naive "global" strategy
  1. Compute $\phi(x, y)$
  2. Compute $t(\phi(x(t), y(t)))$
- Local strategy
  - Write x, y, P_1, P_2, Δ in terms of t
  - Solve for s as a power series in t.
  - Compute ϕ in terms of t

Disadvantage - Has to be done separately for every D_i
Advantage - All computations are with power series in one variable.

Things we don't deal with yet

- How to lift in general from char p to char 0
  (May be enough to find a formal lift)
- How to find a basis of de Rham cohomology
  - It's a problem of computing Riemann-Roch spaces
  - Might be enough to find one element, then use Frobenius to generate other elements.