Computing Zeta Functions of Curves over Finite Fields

Fré Vercauteren

Katholieke Universiteit Leuven

31 July 2008

Algebraic de Rham Cohomology

- Let A be a ring, e.g. the coordinate ring of a curve
- The module of Käher differentials $D^1(A)$ is
- Generated over A by symbols da with $a \in A$ with rules

$$d(a+b) = da + db$$
$$d(a \cdot b) = adb + bda$$

- Elements of dA are called exact

Algebraic de Rham Cohomology

- $\overline{X}$ smooth affine curve over field $\mathbb{K}$ with coordinate ring

$$A = \mathbb{K}[x, y]/(f(x, y))$$

- Since $f(x, y) = 0$ get $(\frac{\partial f}{\partial x}\, dx + \frac{\partial f}{\partial y}\, dy) = 0$, so

$$D^1(A) = \frac{(A\, dx + A\, dy)}{(A(\frac{\partial f}{\partial x}\, dx + \frac{\partial f}{\partial y}\, dy))}$$

- First algebraic de Rham cohomology group is

$$H^1_{DR}(A) = \frac{D^1(A)}{dA}$$

M-W Cohomology of Punctured Affine Line

- Consider $\overline{C} : xy - 1 = 0$ with $\overline{A} = \mathbb{F}_p[x, 1/x]$, then

$$N_r = \#\overline{C}(\mathbb{F}_{p^r}) = p^r - 1$$

- Construct de Rham cohomology in characteristic p?
  - $\Omega^1(\overline{A}) := \overline{A}\, dx/(d\,\overline{A})$ is infinite dimensional.
  - $x^k\, dx$ with $k \equiv -1 \pmod{p}$ cannot be integrated.
- First attempt: lift situation to $\mathbb{Z}_p$ and try again?
  - Consider two lifts to $\mathbb{Z}_p$

$$A_1 = \mathbb{Z}_p[x, 1/x] \quad \text{and} \quad A_2 = \mathbb{Z}_p[x, 1/(x(1 + px))]$$

  - A_1 and A_2 are not isomorphic!
  - $H^1_{DR}(A_1/\mathbb{Q}_p) = \langle \frac{dx}{x} \rangle$ and $H^1_{DR}(A_2/\mathbb{Q}_p) = \langle \frac{dx}{x}, \frac{dx}{1+px} \rangle$.

M-W Cohomology of Punctured Affine Line

- Second attempt: use p-adic completion, then

$$A_1^\infty \cong A_2^\infty \cong \{\sum_{i\in\mathbb{Z}} \alpha_i x^i \in \mathbb{Z}_p[[x, 1/x]] \mid \lim_{i\to\infty} \alpha_i = 0\}$$

- However: $H^1_{DR}(A^\infty/\mathbb{Q}_p)$ is again infinite dimensional!
  - $\sum_i p^i x^{p^i - 1}$ is in A^∞ but integral $\sum_i x^{p^i}$ is not.
- Third attempt: consider the dagger ring or weak completion

$$A^\dagger = \{\sum_{i\in\mathbb{Z}} \alpha_i x^i \in \mathbb{Z}_p[[x, 1/x]] \mid \exists \epsilon \in \mathbb{R}_{>0}, \delta \in \mathbb{R} : v_p(\alpha_i) \geq \epsilon|i| + \delta\}$$

- Note: $A_1^\dagger$ is isomorphic to $A_2^\dagger$, since $1 + px$ invertible in $A_1^\dagger$.

M-W Cohomology of Punctured Affine Line

- M-W cohomology = de Rham cohomology of $A^\dagger \otimes \mathbb{Q}_p$
- $H^1(\overline{A}/\mathbb{Q}_p) = A^\dagger dx/(dA^\dagger)$ and clearly for $k \neq -1$

$$x^k dx = d(\frac{x^{k+1}}{k+1})$$

- Conclusion: $H^1(\overline{A}/\mathbb{Q}_p)$ has basis $\frac{dx}{x}$
- Lifting Frobenius F to $A^\dagger$: infinitely many possibilities

$$F(x) \in x^p + pA^\dagger$$

- Examples: $F_1(x) = x^p$ or $F_2(x) = x^p + p$

M-W Cohomology of Punctured Affine Line

- Action of F_1 on basis $\frac{dx}{x}$ is given by

$$F_1{}^*\left(\frac{dx}{x}\right) = \frac{d(F_1(x))}{F_1(x)} = \frac{d(x^p)}{x^p} = p\frac{dx}{x}$$

- Action of F_2 on basis $\frac{dx}{x}$ is given by

$$F_2{}^*\left(\frac{dx}{x}\right) = \frac{d(F_2(x))}{F_2(x)} = \frac{d(x^p + p)}{x^p + p} = \frac{px^{p-1}}{x^p + p}dx = \frac{p}{1 + px^{-p}}\frac{dx}{x}$$

- Power series: $(1 + px^{-p})^{-1} = \sum_{i=0}^{\infty}(-1)^i p^i x^{-ip} \in A^\dagger$

$$F_2{}^*\left(\frac{dx}{x}\right) = p\frac{dx}{x} + d\left(\sum_{i=1}^{\infty}\frac{(-1)^{i+1}p^{i-1}}{i}x^{-ip}\right)$$

M-W Cohomology of Punctured Affine Line

- Action of F_1 and F_2 are equal on $H^1(\overline{A}/\mathbb{Q}_p)$!

$$F^*(\frac{dx}{x}) = p\frac{dx}{x} \Rightarrow F^{*-1}\left(\frac{dx}{x}\right) = \frac{1}{p}\frac{dx}{x}$$

- Lefschetz Trace formula applied to $\overline{C}$ gives

$$\#\overline{C}(\mathbb{F}_{p^r}) = p^r - \mathrm{Trace}\left((pF^{*-1})^r | H^1(\overline{C}/\mathbb{Q}_p)\right)$$

- Conclusion:

$$\boxed{\#\overline{C}(\mathbb{F}_{p^r}) = p^r - 1}$$

Monsky-Washnitzer Cohomology

- $\overline{X}$ smooth affine curve over field $\mathbb{F}_q$ with coordinate ring

$$\overline{A} = \mathbb{F}_q[x,y]/(\bar{f}(x,y))$$

- Let f be arbitrary lift to $\mathbb{Z}_q$ and let $A = \mathbb{Z}_q[x,y]/(f)$
- Would like to lift the Frobenius endomorphism to A, but in general this is not possible! (cfr. Satoh)
- Working with p-adic completion A^∞ of A does admit lift, but the de Rham cohomology of A^∞ mostly larger than of A.
- For affine line: $\sum p^j x^{p^j-1} dx = d(\sum x^{p^j})$, but $\sum x^{p^j} \notin A^\infty$.
- Problem: series $\sum p^j x^{p^j-1}$ does not converge fast enough for its integral to converge as well.

Dagger rings

- Dagger ring $A^\dagger$ of $A := \mathbb{Z}_q[x, y]/(f)$ is

$$A^\dagger := \mathbb{Z}_q\langle x, y\rangle^\dagger/(f),$$

- $\mathbb{Z}_q\langle x, y\rangle^\dagger$ consists of power series $\sum r_{i,j} x^i y^j \in \mathbb{Z}_q[[x, y]]$

$$\exists\, \delta, \varepsilon \in \mathbb{R}, \varepsilon > 0, \forall (i, j) : \ \mathrm{ord}_p\, r_{i,j} \geq \varepsilon(i + j) + \delta.$$

- Coefficients $r_{i,j}$ get smaller linearly in the degree $i + j$
- The ring $A^\dagger$ satisfies $A^\dagger/pA^\dagger = \overline{A}$
- Only depends up to $\mathbb{Z}_q$-isomorphism on $\overline{A}$
- Admits a lift of the Frobenius endomorphism F_q, since $q = p^n$ we have $F_q = F_p^n$, suffices to lift $F_p =: \Sigma$

p-th Power Frobenius on $A^\dagger$

- Conditions on the p-th power Frobenius Σ on $A^\dagger$ are

$$x^\Sigma \equiv x^p \bmod p \quad \text{and} \quad y^\Sigma \equiv y^p \bmod p \quad \text{and} \quad f^\Sigma(x^\Sigma, y^\Sigma) = 0$$

- Fixing $x^\Sigma = x^p$ also fixes y^Σ since $f^\Sigma(x^p, y^\Sigma) = 0$, thus $\left(\frac{\partial f(x,y)}{\partial y}\right)^p$ has to be invertible in $A^\dagger$.
  - Make $\overline{A}$ larger (i.e. remove points from curve) such that $\partial f(x,y)/\partial y$ invertible in $A^\dagger$
  - Choose more general lift of Frobenius on x, e.g. lift Frobenius on x and y simultaneously such that denominator in the Newton iteration is invertible in $A^\dagger$.

Monsky-Washnitzer Cohomology Groups

- Monksy-Washnitzer = de Rham cohomology of $A^\dagger$

$$H^1(\overline{A}/\mathbb{Q}_q) := D^1(A^\dagger)/d(A^\dagger) \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$$

- $H^1(\overline{A}/\mathbb{Q}_q)$ only depends on $\overline{A}$
- Vectorspace over $\mathbb{Q}_q$ of dimension $2g + m - 1$,
  - g is genus of curve
  - m is the number of missing points

Lefschetz Fixed Point Theorem

- Let $F = \Sigma^n$ be a lift of the q-power Frobenius to $A^\dagger$
- F induces an endomorphism F^* on $H^1(A/\mathbb{Q}_q)$
- Lefschetz fixed point formula: the number of $\mathbb{F}_{q^r}$-rational points on $\overline{X}$ equals

$$q^r - \mathrm{Tr}\left((qF^{*-1})^r | H^1(\overline{A}/\mathbb{Q}_q)\right).$$

- Note: gives number of points over all extensions!

Kedlaya's Algorithm $p > 2$

- Let $y^2 - \overline{f}(x) = 0$ hyperelliptic curve $\overline{C}$ of genus g over $\mathbb{F}_{p^n}$, i.e. $\overline{f}(x)$ of degree $2g + 1$ and squarefree.
- Affine curve $\overline{C}'$ obtained from C by deleting $y = 0$, then coordinate ring $\overline{A} = \mathbb{F}_q[x, y, y^{-1}]/(y^2 - \overline{f}(x))$
- Lift $\overline{C}'$ to C' over $\mathbb{Z}_q$ by taking any lift $f(x) \in \mathbb{Z}_q[x]$ of $\overline{f}(x)$ and removing $y = 0$ of curve defined by $f = 0$.
- Coordinate ring of C' is $A = \mathbb{Z}_q[x, y, y^{-1}]/(y^2 - f(x))$.
- $A^\dagger$ contains series $\sum_{k=-\infty}^{+\infty}(S_k(x) + T_k(x)y)y^{2k}$ with $\deg S_k, \deg T_k \leq 2g$ and valuation of S_k and T_k grows linearly with $|k|$.

Lifting Frobenius to Dagger Ring $A^\dagger$

Lift $\overline{\Sigma}$ to $\Sigma : A^\dagger \longrightarrow A^\dagger$ as

$$x^\Sigma := x^p \quad \text{and} \quad \Sigma(y) \text{ satisfies } (y^\Sigma)^2 = f(x)^\Sigma .$$

Formula for y^Σ as element of $A^\dagger$:

$$\begin{aligned} y^\Sigma &= (f(x)^\Sigma)^{1/2} \\ &= (f(x)^\Sigma - f(x)^p + f(x)^p)^{1/2} \\ &= f(x)^{p/2}(1 + \frac{f(x)^\Sigma - f(x)^p}{f(x)^p})^{1/2} \\ &= y^p \sum_{k=0}^{\infty} \binom{1/2}{k} \frac{\left(f(x)^\Sigma - f(x)^p\right)^k}{y^{2pk}} \end{aligned}$$

Lifting Frobenius to Dagger Ring $A^\dagger$: Practice

- Actually need $(y^\Sigma)^{-1}$, can be computed as $(y^\Sigma)^{-1} = y^{-p}R$
- R is a root of the equation $G(Z) = SZ^2 - 1$ with

$$S = (1 + ((f(x)^\Sigma) - f(x)^p)/y^{2p})$$

- Newton iteration to compute R is given by

$$Z \leftarrow \frac{Z(3 - SZ^2)}{2}$$

  starting from $Z \equiv 1 \pmod p$.
- In each step, the truncated power series should be reduced modulo f

Kedlaya's Algorithm: Differentials

- Since $y^2 - f(x) = 0$, we have $dy = \frac{f'(x)dx}{2y}$ and thus

$$D^1(A^\dagger) = A^\dagger \frac{dx}{y}$$

- Any differential form can thus be written as

$$\sum_{k=-\infty}^{k=+\infty} \frac{h_k(x)}{y^k} dx$$

with $\deg h_k < \deg f$

Kedlaya's Algorithm: Reduction of Differentials

- $h(x)/y^s dx$ with $h(x) \in \mathbb{Q}_q[x]$ and $s \in \mathbb{N}$ can be reduced
- Write $h(x) = U(x)f(x) + V(x)f'(x)$, then

$$\frac{h(x)}{y^s}dx = \frac{U(x)f(x) + V(x)f'(x)}{y^s}dx = \frac{U(x)}{y^{s-2}}dx + \frac{V(x)f'(x)}{y^s}dx$$

- Consider exact differential

$$d(V(x)/y^{s-2}) = \frac{V'(x)}{y^{s-2}}dx - \frac{(s-2)V(x)}{y^{s-1}}dy \equiv 0$$

- Finally we obtain

$$\frac{h(x)}{y^s}dx \equiv \left(U(x) + \frac{2V'(x)}{s-2}\right)\frac{dx}{y^{s-2}}$$

- Reduced to the case $s = 2$ or $s = 1$

Kedlaya's Algorithm: Reduction of Differentials

- $h(x)y^s dx$ with $s \in \mathbb{N}$ even is exact since $h(x)f(x)^{s/2}dx$ is
- $h(x)y^s dx$ with $s \in \mathbb{N}$ for s odd is $\frac{h(x)f(x)^{(s+1)/2}}{y}dx$
- Differential $h(x)/y\,dx$ with $\deg h = n \geq 2g$ can be reduced by subtracting multiples of $d(x^{i-2g}y)$ for $i = n, \ldots, 2g$
- Differential $h(x)/y^2\,dx$ with $\deg h \geq 2g + 1$ is equivalent to $(h(x) \bmod f(x))/y^2 dx$

Kedlaya's Algorithm: Basis for $H^1(\overline{A}/\mathbb{Q}_q)$

- Have shown $H^1(\overline{A}/\mathbb{Q}_q) = H^1(\overline{A}/\mathbb{Q}_q)^+ \oplus H^1(\overline{A}/\mathbb{Q}_q)^-$
  - $H^1(\overline{A}/\mathbb{Q}_q)^+$ generated by $x^i dx/y^2$ for $i = 0, \ldots, 2g$
  - $H^1(\overline{A}/\mathbb{Q}_q)^-$ generated by $x^i dx/y$ for $i = 0, \ldots, 2g-1$
- The invariant part corresponds to the $2g+1$ removed points with y-coordinate zero.
- The characteristic polynomial of F^* on $H^1(\overline{A}/\mathbb{Q}_q)^-$ equals

$$\chi(t) := t^{2g} P(1/t) \text{ with } Z(\overline{C}; t) = \frac{P(t)}{(1-t)(1-qt)}.$$

Computing Action of Frobenius on $H^1(\overline{A}/K)^-$

- The action of Σ^* on a differential form $x^k dx/y$ is given by

$$\Sigma^*(x^k dx/y) \equiv p x^{pk+p-1} dx/\Sigma(y).$$

- Using the equation of the curve and subtracting suitable exact differentials we can express $\Sigma^*(x^k dx/y^l)$ again on $H^1(\overline{A}/K)^-$.
- This gives matrix M which is an approximation of the action of Σ^* on $H^1(\overline{A}/K)^-$.
- The polynomial $\chi(t) := t^{2g} P(1/t)$ can then be approximated by the characteristic polynomial of $M M^{\Sigma} \cdots M^{\Sigma^{n-1}}$.

Kedlaya's Algorithm: Example

- Let $\overline{C}$ be hyperelliptic curve over $\mathbb{F}_3$ defined by

$$y^2 = x^5 + x^4 + 2x^3 + 2x + 2.$$

- The Frobenius on y^{-1} modulo 3^6 is given by $y^{-p} \cdot R$

$$\begin{aligned} R \equiv 1 &+ (-363x^4 + 96x^3 + 144x^2 - 6x + 207)\tau + (-123x^4 - 153x^3 - 21x^2 + 351x + 210)\tau^2 \\ &+ (339x^4 - 228x^3 - 60x^2 - 204x + 186)\tau^3 + (-81x^4 + 54x^3 - 243x^2 - 243x + 27)\tau^4 \\ &+ (-54x^4 - 162x^3 - 54x^2 - 54x + 162)\tau^5 + (351x^4 + 189x^3 + 189x^2 + 189x + 351)\tau^6 \\ &+ (-243x^4 + 243x^3 - 108x^2 - 270x + 27)\tau^7 + (-135x^3 + 54x^2 + 81x - 108)\tau^8 \\ &+ (216x^4 + 108x^3 - 297x^2 + 351x - 162)\tau^9 + (-243x^4 - 162x^3 - 324x^2 + 243x)\tau^{10} \\ &+ (81x^4 - 243x^3 - 162x^2 + 162x - 81)\tau^{11} + (-162x^4 + 162x^3 + 324x^2 - 324x + 324)\tau^{12} \end{aligned}$$

with $\tau = y^{-2}$.

Kedlaya's Algorithm: Example

- The matrix M is given by

$$M = \begin{bmatrix} 27 & 39 & 30 & 108 \\ 129 & 36 & 27 & 126 \\ 204 & 186 & 12 & 138 \\ 46/3 & 76/3 & 41/3 & 169 \end{bmatrix}$$

- $\chi(T) \equiv T^4 + 80T^3 + T^2 + 78T + 9 \pmod{3^4}$, so

$$Z(\tilde{C}/\mathbb{F}_q; T) = \frac{9T^4 - 3T^3 + T^2 - T + 1}{(1-T)(1-3T)}$$

Kedlaya's Algorithm: Final Words

- Complexity for fixed p is $\tilde{O}(g^4 n^3)$
- Dependence on p is $O(p(\log p)^k)$, so fully exponential
- Only practical for moderately small p, e.g. $p \leq 500$
- Harvey's modification: $\tilde{O}(p^{1/2} g^{5.5} n^{3.5} + g^8 n^5 \log p)$
- Characteristic 2 version is more subtle, need special lift of equation of the curve
- Extension to very general class of non-degenerate curves