Computing Zeta Functions of Curves over Finite Fields

Fré Vercauteren

Katholieke Universiteit Leuven

30 July 2008
Introduction

$p$-adic Numbers

Satoh’s Algorithm
The Zeta Function and Weil Conjectures

Let $\overline{C}$ be smooth projective curve over $\mathbb{F}_q$; zeta function of $\overline{C}$ is

$$Z(T) = Z(\overline{C}; T) = \exp \left( \sum_{k=1}^{\infty} N_k \frac{T^k}{k} \right)$$

with $N_k$ the number of points on $\overline{C}$ with coordinates in $\mathbb{F}_{q^k}$.

Weil Conjectures:

- $Z(T)$ is rational function over $\mathbb{Z}$ and can be written as

$$P(T) \frac{1}{(1 - T)(1 - qT)}$$

- $P(T) = \prod_{i=1}^{2g} (1 - \alpha_i T)$ with $g$ genus of $\overline{C}$ and $|\alpha_i| = \sqrt{q}$
- $P(T) = \sum_{i=0}^{2g} a_i T^i$ with $a_0 = 1$, $a_{2g} = q^g$ and $a_{g+i} = q^i a_{g-i}$
Ultimate Goal

- Given $\overline{C}$ over $\mathbb{F}_q$ of genus $g$, compute zeta function efficiently (at least polynomial time) for a bounded range of $q^g \leq 2^{512}$

- $q^g$ roughly the size of the group $J_C(\mathbb{F}_q)$

Current situation:

- Elliptic curves: efficient solution for all $\mathbb{F}_q$
- Hyperelliptic curves: good solution for $\mathbb{F}_{p^n}$ and $p$ small, any genus allowed
- Nondegenerate curves: decent solution for $\mathbb{F}_{p^n}$, $p$ small, small genus
Central Object: Frobenius Endomorphism

- Recall $a \in \overline{F}_q$ is in $F_q$ iff $a^q = a$
- Frobenius automorphism $\varphi_q : \overline{F}_q \to \overline{F}_q : x \mapsto x^q$ induces
  - morphism $\varphi_q$ on $C(\overline{F}_q)$
  - endomorphism $\varphi_q$ on $J_C(\overline{F}_q)$
- $F_q$-rational points are invariant under $\varphi_q$

$$J_C(\overline{F}_q) = \text{Ker}(1 - \varphi_q) \quad \#J_C(\overline{F}_q) = \text{deg}(1 - \varphi_q)$$

- Theorem: $P(T) = \chi(1/T)t^{2g}$
- Remark: for $q = p^n$, then $\varphi_q$ is composition of $n$ morphisms of degree $p$ (easy to handle for $p$ small)
Overview of Existing Approaches

- \( l \)-adic: Schoof’s algorithm and generalisations
  - consider the \( l \)-torsion as first order approximations of \( l \)-adic cohomology (cfr. representation on Tate module)
  - compute characteristic polynomial of Frobenius modulo \( l_i \), for various small \( l_i \) and recover \( \chi(T) \mod \prod_i l_i \).

- \( p \)-adic:
  - canonical lift
  - \( p \)-adic cohomology
  - \( p \)-adic deformation
$p$-adic Numbers

- $p$-adic valuation $\text{ord}_p(r)$ of $r \in \mathbb{Q}$ is $\rho$ with
  \[ r = p^\rho u/v, \quad \rho, u, v \in \mathbb{Z}, \quad p \nmid u, \ p \nmid v \]
- Non-archimedean $p$-adic norm $|r|_p = p^{-\rho}$
- Field of $p$-adic numbers $\mathbb{Q}_p$ is completion of $\mathbb{Q}$ w.r.t. $\cdot |_p$,
  \[ \sum_{m} a_i p^i, \quad a_i \in \{0, 1, \ldots, p - 1\}, \quad m \in \mathbb{Z}. \]
- $p$-adic integers $\mathbb{Z}_p$ is the ring with $| \cdot |_p \leq 1$ or $m \geq 0$.
- Ideal $M = \{ x \in \mathbb{Q}_p \mid |x|_p < 1 \} = p\mathbb{Z}_p$ and $\mathbb{Z}_p/M \cong \mathbb{F}_p$. 
**$p$-adic Numbers in Practice**

- $\mathbb{Z}_p$: for fixed absolute precision $N$, compute modulo $p^N$
- $\mathbb{Q}_p$: write each element as $p^{\text{ord}_p(x)}u_x$ with $u_x \in \mathbb{Z}_p^\times$
- $\mathbb{Q}_p$: for fixed relative precision of $N$, $u_x \mod p^N$
- No rounding off errors occur unlike floating point
- Loss of absolute precision on division by $p$
- Possible loss of relative precision when subtracting
- All operations asymptotically in time $O(N \log p)^{1+\varepsilon}$
- For $\log_2 p^N < 512$, schoolbook methods suffice
Unramified Extensions of $p$-adics

- $K$ extension of $\mathbb{Q}_p$ of degree $n$ with valuation ring $R$ and maximal ideal $M_R = \{ x \in K \mid |x|_p < 1 \}$ of $R$
- $K$ is called unramified iff its residue field $R/M_R \cong \mathbb{F}_q$
- $K$ denoted with $\mathbb{Q}_q$ and its valuation ring with $\mathbb{Z}_q$
- $\text{Gal}(\mathbb{Q}_q/\mathbb{Q}_p) \cong \text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ and $\text{Gal}(\mathbb{F}_q/\mathbb{F}_p) = < \sigma >$ with
  \[
  \sigma : \mathbb{F}_q \to \mathbb{F}_q : x \mapsto x^p
  \]
- $\text{Gal}(\mathbb{Q}_q/\mathbb{Q}_p) = < \Sigma >$ generated by Frobenius substitution
- Note: $\Sigma$ is not simple $p$-powering!
Representation of $\mathbb{Q}_q$

- Let $\mathbb{F}_q \cong \mathbb{F}_p[t]/(\tilde{f}(t))$ then $\mathbb{Q}_q$ can be constructed as $\mathbb{Q}_q \cong \mathbb{Q}_p[t]/(f(t))$, with $f(t)$ any lift of $\tilde{f}(t)$ to $\mathbb{Z}_p[t]$.

- Different choices of $f(t)$ have different advantages.

- Valuation ring $\mathbb{Z}_q \cong \mathbb{Z}_p[t]/f(t)$; $a \in \mathbb{Z}_q$ represented as $a = \sum_{i=0}^{n-1} a_i t^i$, $a_i \in \mathbb{Z}_p$.

- Reduction mod $p^m$ gives $(\mathbb{Z}/p^m\mathbb{Z})[t]/(f_m(t))$ with $f_m(t) \equiv f(t) \mod p^m$. 
Frobenius Substitution

- Let \( \mathbb{Z}_q \cong \mathbb{Z}_p[\theta] \cong \mathbb{Z}_p[t]/(f(t)) \) with \( f(t) = \sum_{i=0}^{n-1} f_i t^i \)

\[
0 = \Sigma(f(\theta)) = \sum_{i=0}^{n-1} f_i \Sigma(\theta)^i = f(\Sigma(\theta)).
\]

- Compute \( \Sigma(\theta) \) as zero of \( f(t) \) from \( \Sigma(\theta) \equiv \theta^p \mod p \).

- Frobenius of \( a = \sum_{i=0}^{n-1} a_i \theta^i \in \mathbb{Q}_q \) is \( \Sigma(a) = \sum_{i=0}^{n-1} a_i \Sigma(\theta)^i \)

- If \( \theta \) is \( (q - 1) \)-th root of unity (Teichmüller lift), then \( \Sigma(\theta) = \theta^p \)

- Occurs when \( f(t) \mid t^q - t \), i.e. is Teichmüller modulus
Newton Lifting

Theorem: Let $g \in \mathbb{Z}_q[X]$ and assume that $a \in \mathbb{Z}_q$ satisfies

$$\text{ord}_p(g'(a)) = k \text{ and } \text{ord}_p(g(a)) = n + k$$

for some $n > k$, then exists a unique root $b \in \mathbb{Z}_q$ of $f$ with $b \equiv a \pmod{p^n}$.

$a$ is called an approximate root of $g$ known to precision $n$.

Newton iteration: compute

$$z = a - \frac{g(a)}{g'(a)}$$

then $z \equiv b \pmod{p^{2n-k}}$, $g(z) \equiv 0 \pmod{p^{2n}}$ and $\text{ord}_p(g'(z)) = k$. 
Newton Lifting: Minimal Precision

- \( z \) has to be correct modulo \( p^{2n-k} \)
- \( g'(a) \mod p^n \), so \( g'(a)/p^k \) is a unit known \( \mod p^{n-k} \)
- \( g(a) \mod p^{2n} \), then \( g(a) \equiv 0 \mod p^{n+k} \) and \( g(a)/p^{n+k} \) known \( \mod p^{n-k} \)
- Finally compute

\[
z \equiv a - p^n \frac{g(a)/p^k}{g'(a)/p^k} \mod p^{2n-k}
\]

where inversion and multiplication is computed \( \mod p^{n-k} \)
Frobenius Endomorphism

- Let $E$ be an elliptic curve over a finite field $\mathbb{F}_q$ with $q = p^n$
- Recall the $q$-th power Frobenius endomorphism
  
  \[ \varphi_q : E \to E : (x, y) \mapsto (x^q, y^q) \]

- Characteristic polynomial of $\varphi_q$ was of the form
  
  \[ \chi(T) = T^2 - \text{Tr}(\varphi_q)T + \text{Deg}(\varphi_q) = T^2 - tT + q \]

  and $\#E(\mathbb{F}_q) = \chi(1) = q + 1 - t$
Factorisation of $\chi(T)$ over $p$-adic’s

- $\mathbb{Q}_p$ is field of $p$-adic numbers, with valuation ring $\mathbb{Z}_p$
- Assume that $t \not\equiv 0 \mod p$, then
  \[ \chi(T) \equiv T^2 - tT \equiv T(T - t) \mod p \]
- Conclusion: $\chi(T)$ splits over $\mathbb{Z}_p$ as
  \[ \chi(T) = (T - \lambda)(T - \frac{q}{\lambda}) \]
  with $\lambda$ the unique root such that $\lambda \equiv t \mod p$ ($\lambda$ is unit)
- Conclusion: $t = \lambda + q/\lambda$, since $|t| \leq 2\sqrt{q}$ only need approximation of $\lambda$ modulo $p^N$ with $N > n/2 + 2$
How to Compute $\lambda$?

- Since $\lambda \in \mathbb{Z}_p$, need to lift the situation to $p$-adic integers
- Given elliptic curve $E$ over $\mathbb{F}_q$, can we find $\mathcal{E}$ over $\mathbb{Z}_q$ s.t.
- Reduction of $\mathcal{E}$ modulo $p$ equals $E$
- $\mathcal{E}$ comes with “lifted Frobenius endomorphism $\mathcal{F}_q$” with the same characteristic polynomial
  \[ \chi(\varphi_q; T) = \chi(\mathcal{F}_q; T) \]
- Assume that we could compute $\mathcal{E}$ and $\mathcal{F}_q$, then how to proceed?
How to Compute $\lambda$?

- Let $E : f(x, y) = 0$ over field $\mathbb{K}$, then there exists an invariant differential

$$\omega = \frac{dx}{\partial f/\partial y}$$

- Morphism $\phi : E_1 \rightarrow E_2$ induces by pullback a map $\Omega_2 \rightarrow \Omega_1$

$$\phi^*(gdh) = \phi^*(g)d\phi^*(h) = (g \circ \phi)d(h \circ \phi)$$

- Invariant: since $\tau_P^*\omega = \omega$

- Linearization: $\phi, \psi$ 2 isogenies from $E_1 \rightarrow E_2$ then

$$(\phi \oplus \psi)^*\omega = \phi^*\omega + \psi^*\omega$$

- Pullback of regular differential by isogeny again regular, so

$$\phi^*\omega = c\omega, \; c \in \mathbb{K}$$
How to Compute $\lambda$?

- Since $F_q$ satisfies $T^2 - tT + q = 0$, the constant $F_q^*\omega = c\omega$ satisfies
  \[ c^2 - tc + q = 0 \]

- Conclusion: $c$ is either $\lambda$ or $q/\lambda$ but which one?
- Use that $F_q \equiv \varphi_q \mod p$ and clearly $\varphi_q^*\bar{\omega} \equiv 0 \mod p$, so
  \[ c = \frac{q}{\lambda} \]

- Efficiency: would need extra $n$ precision to recover $\lambda$ and trace $t$
- Solution: consider the dual $\hat{F}_q$ of $F_q$, then $\hat{F}_q^*\omega = \lambda\omega$
Canonical Lift

- The canonical lift $\mathcal{E}$ of an ordinary elliptic curve $E$ over $\mathbb{F}_q$ is an elliptic curve over $\mathbb{Q}_q$ which satisfies:
- the reduction of $\mathcal{E}$ modulo $p$ equals $E$,
- the ring homomorphism $\text{End}(\mathcal{E}) \rightarrow \text{End}(E)$ induced by reduction modulo $p$ is an isomorphism.
- Deuring showed that the canonical lift $\mathcal{E}$ always exists and is unique up to isomorphism.
Canonical Lift: Alternative Characterisation

- $\mathcal{E}$ is the canonical lift of $E$.
- Reduction modulo $p$ induces an isomorphism $\text{End}(\mathcal{E}) \simeq \text{End}(E)$.
- The $q$-th power Frobenius $F_q \in \text{End}(E)$ lifts to an endomorphism $\mathcal{F}_q \in \text{End}(\mathcal{E})$.
- The $p$-th power Frobenius isogeny $F_p : E \to E^\sigma$ lifts to an isogeny $\mathcal{F}_p : \mathcal{E} \to \mathcal{E}^\Sigma$, with $\Sigma$ the Frobenius substitution.

Conclusion: last property implies that the $j$-invariant of $\mathcal{E}$ has to satisfy

$$\Phi_p(j(\mathcal{E}), \Sigma(j(\mathcal{E}))) = 0$$
Let $E$ be an ordinary elliptic curve over $\mathbb{F}_q$ with $j$-invariant $j(E) \in \mathbb{F}_q \setminus \mathbb{F}_{p^2}$.

Then the system of equations

$$\Phi_p(X, \Sigma(X)) = 0 \text{ and } X \equiv j(E) \pmod{p},$$

has a unique solution $J \in \mathbb{Z}_q$, which is the $j$-invariant of the canonical lift $\mathcal{E}$ of $E$ (defined up to isomorphism).

**Example:** $\Phi_2(X, Y) = X^3 + Y^3 - X^2Y^2 + 1488(XY^2 + X^2Y) - 162000(X^2 + Y^2) + 4077375XY + 8748000000(X + Y) - 157464000000000$

When $j(E) \in \mathbb{F}_{p^2}$, then isomorphic to curve over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$, so can use simple enumeration.
Canonial Lift: Satoh’s Algorithm

- To compute $j(E) \mod p^N$, Satoh considered $E$ together with all its conjugates $E_i = E^{\sigma^i}$ with $0 \leq i < n$
- Let $F_{p,i}$ denote the $p$-th power Frobenius isogeny, then
  \[ E_0 \xrightarrow{F_{p,0}} E_1 \xrightarrow{F_{p,1}} \ldots \xrightarrow{F_{p,n-2}} E_{n-1} \xrightarrow{F_{p,n-1}} E_0. \]
- Satoh lifts cycle $(E_0, E_1, \ldots, E_{n-1})$ simultaneously
Canonical Lift: Weierstrass Model

\[ p = 2 \quad : \quad y^2 + xy = x^3 + a_6, \quad j(E) = 1/a_6 \]
\[ p = 3 \quad : \quad y^2 = x^3 + x^2 + a_6, \quad j(E) = -1/a_6 \]
\[ p > 5 \quad : \quad y^2 = x^3 + 3ax + 2a, \quad j(E) = 1728a/(1 + a) \]

Given \( j \)-invariant \( j(\mathcal{E}) \) of the canonical lift of \( E \), a Weierstrass model for \( \mathcal{E} \) is given by

\[ p = 2 \quad : \quad y^2 + xy = x^3 + 36\alpha x + \alpha, \quad \alpha = 1/(1728 - j(\mathcal{E})) \]
\[ p = 3 \quad : \quad y^2 = x^3 + x^2/4 + 36\alpha x + \alpha, \quad \alpha = 1/(1728 - j(\mathcal{E})) \]
\[ p > 5 \quad : \quad y^2 = x^3 + 3\alpha x + 2\alpha, \quad \alpha = j(\mathcal{E})/(1728 - j(\mathcal{E})) \]
How to compute $\lambda$?

- From before: the dual $\hat{F}_q$ of $F_q$, then $\hat{F}_q^* \omega = \lambda \omega$

- The diagram implies

$$\hat{F}_q = \hat{F}_{p,0} \circ \hat{F}_{p,1} \circ \cdots \circ \hat{F}_{p,n-1}$$

- Consider $\omega_i = \omega^{\sum^i}$ for $0 \leq i < n$ and let $c_i$ be defined by

$$\hat{F}_{p,i}^*(\omega_i) = c_i \omega_{i+1},$$

- Conclusion: $\lambda = \prod_{0 \leq i < d} c_i$

- Commutative squares are conjugates, so $c_i = \Sigma^i(c_0)$ and

$$\lambda = \text{No}_{\mathbb{Q}_q/\mathbb{Q}_p}(c_0)$$
How to compute $c_0$?

- Know equations of $\mathcal{E}_0$ and $\mathcal{E}_1$, assume we know $\text{Ker}(\hat{F}_{p,0})$
- Vélu's formulas: compute an equation of $\mathcal{E}_1/\text{Ker}(\hat{F}_{p,0})$ and isogeny $\nu_0$
- Since $\text{Ker}(\nu_0) = \text{Ker}(\hat{F}_{p,0})$, there exists an isomorphism $\lambda_0 : \mathcal{E}_1/\text{Ker}(\hat{F}_{p,0}) \to \mathcal{E}_0$ that makes diagram commutative
How to compute $c_0$?

Vélu’s construction: chooses holomorphic differential such that action of $\nu_0$ is trivial

Conclusion: it is sufficient to compute the action of $\lambda_0$ on $\omega_0$
Computing $\text{Ker}(\widehat{F}_{p,0})$?

- Note that $\text{Ker}(\widehat{F}_{p,0})$ is a subgroup of order $p$ of $\mathcal{E}_1[p]$.
- Let $H_0(x)$ be $H_0(x) = \prod_{P \in (\text{Ker}(\widehat{F}_{p,0}) \setminus \{O\})/\pm} (x - x(P))$.
- $H_0(x)$ divides the $p$-division polynomial $\Psi_{p,1}(x)$ of $\mathcal{E}_1$.
- Lemma: $H_0(x) \in \mathbb{Z}_q[x]$ is the unique monic polynomial that divides $\Psi_{p,1}(x)$ and such that $H_0(x)$ is squarefree modulo $p$ of degree $(p - 1)/2$.
- Need to modify Hensel since reduction mod $p$ of $H_0(x)$ not coprime with $\Psi_{p,1}$.
How to compute $c_0$?

- For $p > 3$, $\mathcal{E}_1$ has equation $y^2 = x^3 + a_1 x + b_1$
- Vélu: $\mathcal{E}_1/\text{Ker}(\hat{F}_{p,0})$ has equation $y^2 = x^3 + \alpha_1 x + \beta_1$

\[
\alpha_1 = (6 - 5p)a_1 - 30(h^2_{0,1} - 2h_{0,2})
\]
\[
\beta_1 = (15 - 14p)b_1 - 70(-h^3_{0,1} + 3h_{0,1} h_{0,2} - 3h_{0,3}) + 42a_1 h_{0,1}
\]

where $h_{0,k}$ is coefficient of $x^{(p-1)/2-k}$ in $H_0(x)$

- $\lambda_0$ to $\mathcal{E}_0 : y^2 = x^3 + a_0 x + b_0$ is $\lambda_0 : (x, y) \rightarrow (u_0^2 x, u_0^3 y)$ with

\[
u_0^2 = \frac{\alpha_1}{\beta_1} \frac{b_0}{a_0}
\]

- Let $\omega_0 = dx/y$ then $\lambda_0^*(\omega_0) = u_0^{-1} \omega_{1,K}$ with $\omega_{1,K} = dx/y$

- Conclusion: $c_0 = u_0^{-1}$
Satoh’s Algorithm: Example

- Let $p = 5$, $d = 7$, $\mathbb{F}_{p^d} \simeq \mathbb{F}_p(\theta)$ with $\theta^7 + 3\theta + 3 = 0$
- Elliptic curve $E : y^2 = x^3 + x + a_6$

$$a_6 = 4\theta^6 + 3\theta^5 + 3\theta^4 + 3\theta^3 + 3\theta^2 + 3.$$  

- The $j$-invariant of canonical lift with precision 6 then is

$$J_0 \equiv 6949 T^6 + 6806 T^5 + 14297 T^4 + 2260 T^3 + 13542 T^2 + 13130 T + 15215,$$

with $\mathbb{Z}_q \simeq \mathbb{Z}_p[T]/(G(T))$ and $G(T) = T^7 + 3T + 3$.

- Values for $a$, $b$ of $\mathcal{E} : y^2 = x^3 + ax + b$

$$a \equiv 6981 T^6 + 8408 T^5 + 1033 T^4 + 8867 T^3 + 15614 T^2 + 3514 T + 675$$
$$b \equiv 4654 T^6 + 397 T^5 + 5897 T^4 + 703 T^3 + 5201 T^2 + 7551 T + 450$$
Satoh’s Algorithm: Example

- Polynomial $H$ describing the kernel of $F_p$

$$H(x) \equiv x^2 + (1395 T^6 + 7906 T^5 + 3737 T^4 + 9221 T^3 + 9207 T^2 + 5403 T + 7401)x$$
$$+ 6090 T^6 + 206 T^5 + 5259 T^4 + 7576 T^3 + 3863 T^2 + 8903 T + 7926$$

- Recover $\alpha$ and $\beta$ as

$$\alpha \equiv 11086 T^6 + 2618 T^5 + 6983 T^4 + 13192 T^3 + 15324 T^2 + 13544 T + 10550 T + 12470$$
$$\beta \equiv 4940 T^6 + 3060 T^5 + 14966 T^4 + 6589 T^3 + 7934 T^2 + 6060 T + 12470$$

- Norm of $(\alpha b)/(\beta a)$ and taking the square root,

$$\text{Tr}(\varphi_q) = 433 \quad \text{and} \quad |E(\mathbb{F}_p^2)| = 77693$$
Computing Zeta Functions of Curves over Finite Fields

Fré Vercauteren

Katholieke Universiteit Leuven

31 July 2008
Algebraic de Rham Cohomology

Example of Punctured Affine Line

Monsky-Washnitzer Cohomology

Kedlaya’s Algorithm for $p > 2$
Algebraic de Rham Cohomology

- Let $A$ be a ring, e.g. the coordinate ring of a curve
- The module of Kähler 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

$$H_{DR}^1(A) = \frac{D^1(A)}{dA}$$
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
  \[ A_1^\infty \cong A_2^\infty \cong \left\{ \sum_{i \in \mathbb{Z}} \alpha_i x^i \in \mathbb{Z}_p[[x, 1/x]] \mid \lim_{i \to \infty} \alpha_i = 0 \right\} \]

- However: $H_{DR}^1(A^\infty / \mathbb{Q}_p)$ is again infinite dimensional!
  - $\sum_i p^i x^{p^i-1}$ is in $A^\infty$ but integral $\sum_i x^{p^i}$ is not.

- Third attempt: consider the dagger ring or weak completion
  \[ A_1^+ = \left\{ \sum_{i \in \mathbb{Z}} \alpha_i x^i \in \mathbb{Z}_p[[x, 1/x]] \mid \exists \epsilon \in \mathbb{R}_{>0}, \delta \in \mathbb{R} : v_p(\alpha_i) \geq \epsilon |i| + \delta \right\} \]

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

\[
x^k dx = d\left(\frac{x^{k+1}}{k+1}\right)
\]

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

$$F_2^* \left( \frac{dx}{x} \right) = p \frac{dx}{x} + d \left( \sum_{i=1}^{\infty} (-1)^{i+1} p^{i-1} x^{-ip} \right)$$
M-W Cohomology of Punctured Affine Line

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

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

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

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

- Conclusion:

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

- $\overline{X}$ smooth affine curve over field $\mathbb{F}_q$ with coordinate ring
  
  $$\overline{A} = \mathbb{F}_q[x, y]/(\overline{f}(x, y))$$

- 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 $A^\infty$ of $A$ does admit lift, but the de Rham cohomology of $A^\infty$ mostly larger than of $A$.

- For affine line: $\sum p^j x^{p^j-1} dx = d(\sum x^{p^j})$, but $\sum x^{p^j} \not\in A^\infty$.

- 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 $\sum r_{i,j} x^i y^j \in \mathbb{Z}_q[[x, y]]$
  \[ \exists \delta, \varepsilon \in \mathbb{R}, \varepsilon > 0, \forall (i, j) : \text{ord}_p r_{i,j} \geq \varepsilon (i + j) + \delta. \]
- 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 \( \Sigma \) on \( A^\dagger \) are
  \[
  x^\Sigma \equiv x^p \mod p \quad \text{and} \quad y^\Sigma \equiv y^p \mod p \quad \text{and} \quad f^\Sigma(x^\Sigma, y^\Sigma) = 0
  \]

- Fixing \( x^\Sigma = x^p \) also fixes \( y^\Sigma \) since \( f^\Sigma(x^p, y^\Sigma) = 0 \), thus
  \[
  \left( \frac{\partial f(x, y)}{\partial y} \right)^p \quad \text{has to be invertible in} \quad A^\dagger.
  \]
  - Make \( \bar{A} \) 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

- Monsky-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
  \[ q^r - \text{Tr} \left( (qF^* - 1)^r | H^1(\overline{A}/\mathbb{Q}_q) \right). \]
- Note: gives number of points over all extensions!
Kedlaya’s Algorithm $p > 2$

- Let $y^2 - \bar{f}(x) = 0$ hyperelliptic curve $\bar{C}$ of genus $g$ over $\mathbb{F}_{p^n}$, i.e. $\bar{f}(x)$ of degree $2g + 1$ and squarefree.

- Affine curve $\bar{C}'$ obtained from $C$ by deleting $y = 0$, then coordinate ring $\bar{A} = \mathbb{F}_q[x, y, y^{-1}]/(y^2 - \bar{f}(x))$

- Lift $\bar{C}'$ to $C'$ over $\mathbb{Z}_q$ by taking any lift $f(x) \in \mathbb{Z}_q[x]$ of $\bar{f}(x)$ 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 $\sum_{k=-\infty}^{+\infty} \left(S_k(x) + T_k(x)y\right)y^{2k}$ 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 $\Sigma$ 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 $y^\Sigma$ as element of $A^\dagger$: 

\[
y^\Sigma = (f(x)^\Sigma)^{1/2} \\
= (f(x)^\Sigma - f(x)^p + f(x)^p)^{1/2} \\
= f(x)^{p/2}(1 + c)^{1/2} \\
= y^p \sum_{k=0}^{\infty} \binom{1/2}{k} \frac{(f(x)^\Sigma - f(x)^p)^k}{y^{2pk}}
\]
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
  \[
  d\left(\frac{V(x)}{y^{s-2}}\right) = \frac{V'(x)}{y^{s-2}} dx - \frac{(s - 2)V(x)}{y^{s-1}} dy \equiv 0
  \]
- 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 $(h(x) \mod f(x))/y^2 dx$
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 $\Sigma^*$ on a differential form $x^k dx/y$ is given by
  \[ \Sigma^*(x^k dx/y) \equiv px^{pk+p-1} dx/\Sigma(y). \]

- 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 $\Sigma^*$ on $H^1(\overline{A}/K)^-.$

- The polynomial $\chi(t) := t^{2g} P(1/t)$ can then be approximated by the characteristic polynomial of $MM^\Sigma \cdots M^{\Sigma^{n-1}}$. 
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 \( y^{-p} \cdot R \)

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

  with \( \tau = y^{-2} \).
Kedlaya’s Algorithm: Example

- The matrix $M$ is given by

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

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