Zeta Functions: the $p$-adic approach

Frederik Vercauteren
frederik@cs.bris.ac.uk
University of Bristol
Overview

- Zeta functions and Weil conjectures
- Computational approaches
- A nice $p$-adic cohomology theory for the affine line
- Monsky-Washnitzer cohomology
- An algorithm for $C_{a,b}$ curves
- Experimental results
- Conclusions and open problems
The Zeta Function and Weil Conjectures

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

$$Z(t) = Z(\overline{C}; t) = \exp \left( \sum_{r=1}^{\infty} N_r \frac{t^r}{r} \right)$$

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

Weil Conjectures:

- $Z(t)$ is rational function over $\mathbb{Z}$ and can be written as $\frac{P(t)}{(1-t)(1-qt)}$
- $P(t) = \prod_{i=1}^{2g} (1 - \alpha_i t)$ 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 $a_{g+i} = q^i a_{g-i}$
- $N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r$ and $P(1)$ is the order of $\text{Jac}(\overline{C}/\mathbb{F}_q)$
Computational Approaches

- **$l$-adic** compute zeta function mod small primes $l \neq p$ + CRT.
  - Need explicit description of $l$-torsion of abelian variety
  - Practical for genus 1 and 2 curves (Schoof, Pila, A-H, …)

- **$p$-adic** compute zeta function mod high power of $p$
  - Canonical Lift / AGM:
    * Ordinary abelian varieties admitting lift of Frobenius
    * Compute action of Frobenius on invariant differential forms
    * Elliptic curves over $\mathbb{F}_p^n$: Satoh, Mestre, …
    * Hyperelliptic curves over $\mathbb{F}_{2^n}$: Mestre
  - $p$-adic Cohomology
### Computational Approaches: Complexity

<table>
<thead>
<tr>
<th>Approach</th>
<th>$p$</th>
<th>$n$</th>
<th>genus</th>
</tr>
</thead>
<tbody>
<tr>
<td>$l$-adic</td>
<td>polylog</td>
<td>polynomial</td>
<td>$\geq$ exponential</td>
</tr>
<tr>
<td>$p$-adic canonical lift</td>
<td>polynomial</td>
<td>$\geq$ quadratic</td>
<td>exponential</td>
</tr>
<tr>
<td>$p$-adic cohomology</td>
<td>linear</td>
<td>$\geq$ cubic</td>
<td>polynomial</td>
</tr>
</tbody>
</table>
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 $R/M_R \cong \mathbb{F}_q$.

- Let $\mathbb{F}_q \cong \mathbb{F}_p[t]/(\overline{Q}(t))$ then $\mathbb{Q}_q$ can be constructed as

$$
\mathbb{Q}_q \cong \mathbb{Q}_p[t]/(Q(t)),
$$

with $Q(t)$ any monic lift of $\overline{Q}(t)$ to $\mathbb{Z}_p[t]$.

- $\text{Gal}(\mathbb{Q}_q/\mathbb{Q}_p)$ is cyclic with generator Frobenius substitution $\sigma$ and $\sigma$ modulo $p$ equals $p$-th power Frobenius $\overline{\sigma}$ on $\mathbb{F}_q$.

- Since $q = p^n$ we have $F = \sigma^n$ and $\overline{F}$ is $q$-th power Frobenius.
Computing Zeta Function - General Strategy

- $\overline{X}$ smooth affine variety over $\mathbb{F}_q$ of dimension $d$.

- Monsky and Washnitzer construct $\mathbb{Q}_q$-vectorspaces $H^i(\overline{X}/\mathbb{Q}_q)$ with an induced action of Frobenius $F_*$ on it such that these cohomology groups satisfy a Lefschetz trace formula:

$$N_r = \sum_{i=0}^{d} (-1)^i \text{Tr} ((q^d F_*^{-1})^r| H^i(\overline{X}/\mathbb{Q}_q))$$

- For smooth affine curve $\overline{C}$ the only non-trivial MW cohomology groups are $H^0(\overline{C}/\mathbb{Q}_q)$ and $H^1(\overline{C}/\mathbb{Q}_q)$, so

$$\#\overline{C}(\mathbb{F}_q^r) = q^r - \text{Trace} ((qF_*^{-1})^r| H^1(\overline{C}/\mathbb{Q}_q))$$
Algebraic de Rham Cohomology

- $X$ smooth, affine variety over $K$ of char 0 with coordinate ring

\[ A := K[x_1, \ldots, x_n]/(f_1, \ldots, f_m) \]

- Module of Kähler differentials $\Omega^1_{A/K}$ generated by $dg$ with $g \in A$

\[ \Omega^1_{A/K} = (A \, dx_1 + \cdots + A \, dx_n)/(\sum_{i=1}^{m} A(\frac{\partial f_i}{\partial x_1} \, dx_1 + \cdots + \frac{\partial f_i}{\partial x_n} \, dx_n)) \] .

- $\Omega^i_{A/K} = \wedge^i \Omega^1_{A/K}$ and $d_i : \Omega^i_{A/K} \to \Omega^{i+1}_{A/K}$ exterior diff.

- Since $d_{i+1} \circ d_i = 0$ we get the de Rham complex $\Omega_{A/K}$

\[ 0 \longrightarrow A \xrightarrow{d_0} \Omega^1_{A/K} \xrightarrow{d_1} \Omega^2_{A/K} \xrightarrow{d_2} \Omega^3_{A/K} \cdots \]
• $i$-th de Rham cohomology group of is defined as

$$H_{DR}^i(A/K) := \text{Ker } d_i / \text{Im } d_{i-1}$$
M-W Cohomology of Affine Line

- Consider $C : xy - 1 = 0$ with coordinate ring $\bar{A} = \mathbb{F}_p[x, 1/x]$, then
  $$N_r = \#C(\mathbb{F}_p^r) = p^r - 1$$

- Construct de Rham cohomology in characteristic $p$?
  - $\Omega^1(\bar{A}) := \bar{A} \, dx/(d \bar{A})$ 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; $1 + px$ not invertible in $A_1$.
  - $H^1_{DR}(A_1/\mathbb{Q}_p) = \langle \frac{dx}{x} \rangle$ and $H^1_{DR}(A_2/\mathbb{Q}_p) = \langle \frac{dx}{x}, \frac{dx}{1+px} \rangle$. 
M-W COHOMOLOGY OF 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: $H^{1}_{DR}(A^\infty / \mathbb{Q}_p)$ 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

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

- Note: $A_1^\dagger$ is isomorphic to $A_2^\dagger$, since $1 + px$ invertible in $A_1^\dagger$. 
M-W Cohomology of Affine Line

• Monsky-Washnitzer 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 AFFINE LINE

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

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

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

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

\[ \#\overline{C}(\mathbb{F}_{p^r}) = p^r - \text{Trace} \left( (pF_*^{-1})^r | H^1(\overline{C}/\mathbb{Q}_p) \right) \]

- Conclusion:

\[ \#\overline{C}(\mathbb{F}_{p^r}) = p^r - 1 \]
**Monsky-Washnitzer cohomology**

- $\overline{X}$ smooth affine variety over $\mathbb{F}_q$ with coordinate ring $\overline{A}$.
- Exists $A := \mathbb{Z}_q[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$ with $A \otimes_{\mathbb{Z}_q} \mathbb{F}_q \cong \overline{A}$
- Dagger ring or weak completion $A^\dagger$ is defined
  \[ A^\dagger := \mathbb{Z}_q\langle x_1, \ldots, x_n \rangle^\dagger/(f_1, \ldots, f_m) \]
  with $\mathbb{Z}_q\langle x_1, \ldots, x_n \rangle^\dagger$ overconvergent power series
  \[ \left\{ \sum_I a_I x^I \in \mathbb{Z}_q[[x_1, \ldots, x_n]] \mid \liminf_{|I| \to \infty} \frac{v_p(\alpha I)}{|I|} > 0 \right\} \]
- M-W cohomology is the de Rham cohomology of $A^\dagger \otimes \mathbb{Q}_q$. 

15
Monsky-Washnitzer cohomology

- Definition only depends on $\overline{A}$ and not on choices made!
- Every morphism $\overline{G} : \overline{A} \to \overline{B}$ lifts to $G : A^{\dagger} \to B^{\dagger}$.
- Induced map on $H^i(\overline{A}/\mathbb{Q}_q) \to H^i(\overline{B}/\mathbb{Q}_q)$ only depends on $\overline{G}$.
- Cohomology groups $H^i(\overline{A}/\mathbb{Q}_q)$ are finite dimensional.
- Let $\overline{C}$ be a projective, smooth curve of genus $g$ over $\mathbb{F}_q$.
  - $S$ a set of $m \mathbb{F}_q$-points and $\overline{A}$ coordinate ring of $\overline{C} \setminus S$
  
  \[
  \dim H^1(\overline{A}/\mathbb{Q}_q) = 2g + m - 1
  \]
\( C_{a,b} \) CURVES

- \( C_{a,b} \) curve \( \overline{C} \) over finite field \( \mathbb{F}_q \),

\[
\overline{C} : y^a + \sum_{i=1}^{a-1} \overline{f}_i(x)y^i + \overline{f}_0(x) = 0
\]

where \( \deg \overline{f}_0(x) = b \), \( a \deg \overline{f}_i(x) + bi \leq ab \) and \( \gcd(a, b) = 1 \).

- Absolutely irreducible and genus is \( g = \frac{(a-1)(b-1)}{2} \).

- Unique degree 1 place \( Q \) at infinity and \( v_Q(x) = -a \), \( v_Q(y) = -b \).

- Various subclasses of \( C_{a,b} \) curves:
  - Hyperelliptic curves: \( a = 2 \) and \( b = 2g + 1 \)
  - Superelliptic curves: \( \overline{f}_i(x) = 0 \) for \( i = 1, \ldots, a - 1 \)
\(C_{a,b} \text{ curves - Lift of Curve}\)

- The affine curve \(\overline{C}\) has coordinate ring \(\overline{A} := \mathbb{F}_q[x, y]/(\overline{C})\).

- Take arbitrary lifts \(f_i(x) \in \mathbb{Z}_q[x]\) of \(\overline{f}_i(x)\) for \(i = 0, \ldots, a-1\) with \(\deg f_i(x) = \deg \overline{f}_i(x)\) and define

\[
C : y^a + \sum_{i=1}^{a-1} f_i(x)y^i + f_0(x) = 0
\]

- Let \(A^\dagger\) be the dagger ring of \(A := \mathbb{Z}_q[x, y]/(C)\).

- Elements of \(A^\dagger\) can be represented as \(\sum_{l=0}^{a-1} \sum_{k=0}^{+\infty} a_{k,l}x^ky^l\) and the valuation of \(a_{k,l}\) grows linearly with \(k\).
$C_{a,b}$ curves - Frobenius on $A^\dagger$

- The necessary conditions on the Frobenius $\sigma$ on $A^\dagger$ are

\[ x^\sigma \equiv x^p \mod p \quad \text{and} \quad y^\sigma \equiv y^p \mod p \quad \text{and} \quad C^\sigma(x^\sigma, y^\sigma) = 0 \]

- Fixing $x^\sigma = x^p$ also fixes $y^\sigma$ as the solution of $C^\sigma(x^p, y^\sigma) = 0$, which implies that \( \left( \frac{\partial C(x, y)}{\partial y} \right)^p \) has to be invertible in $A^\dagger$.

- **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 $x^\sigma = x^p + \alpha Z$ and $y^\sigma = y^p + \beta Z$, then

\[ C^\sigma(x^\sigma, y^\sigma) = C^\sigma(x^p + \alpha Z, y^p + \beta Z) = 0 \quad \text{and} \quad Z \equiv 0 \mod p \]
\( C_{a,b} \) curves - Frobenius on \( A^\dagger \)

- Let \( G(Z) := C^\sigma(x^p + \alpha Z, y^p + \beta Z) \), then \( Z_{k+1} = Z_k - \frac{G(Z_k)}{G'(Z_k)} \) with

\[
G'(Z) \equiv \alpha \frac{\partial C^\sigma}{\partial x} \bigg|_{(x^p, y^p)} + \beta \frac{\partial C^\sigma}{\partial y} \bigg|_{(x^p, y^p)} + O(Z) \mod p
\]

- \( G'(Z) \) will be invertible in \( A^\dagger \) if \( G'(Z) \equiv 1 \mod p \) and thus

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

- Assume \( \overline{C} \) non-singular, then \( \frac{\partial \overline{C}}{\partial x}, \frac{\partial \overline{C}}{\partial y} \) and \( \overline{C} \) generate unit ideal and using Buchberger’s algorithm we compute \( \overline{\alpha}, \overline{\beta}, \overline{\gamma} \in \overline{A} \) with

\[
1 = \overline{\alpha} \left( \frac{\partial \overline{C}}{\partial x} \right)^p + \overline{\beta} \left( \frac{\partial \overline{C}}{\partial y} \right)^p + \overline{\gamma \overline{C}}
\]
$C_{a,b}$ CURVES - BASIS OF $H^1(\overline{A}/\mathbb{Q}_q)$

• If $\overline{C}$ is smooth, then $2g = (a - 1)(b - 1)$ and a basis for $H^1(\overline{A}/\mathbb{Q}_q)$

\[
x^k y^l \, dx \quad \text{for} \quad k = 0, \ldots, b - 2 \text{ and } l = 1, \ldots, a - 1
\]

• Using equation of the curve: $x^i y^l \, dx$ or $x^i y^l \, dy$ for $0 \leq l < a$

• Clearly $d(x^i y^{l+1}) \equiv 0$ and thus $x^i y^l \, dy \equiv -\frac{1}{l+1} x^{i-1} y^l \, dx$

• Differentiating the curve $C$ leads to the equality

\[
\left(\sum_{i=1}^{a-1} f'_i(x) y^i + f'_0(x)\right) \, dx = -(ay^{a-1} + \sum_{i=1}^{a-1} f_i(x) iy^{i-1}) \, dy
\]
\section*{C_{a,b} curves - Reduction Formula}

- To reduce \( x^i y^l \, dx \) we multiply this equation with \( x^j y^l \)

\[
x^j \left( \sum_{i=1}^{a-1} f_i'(x) y^i + f_0'(x) \right) y^l \, dx = -x^j \left( a y^{a-1} + \sum_{i=1}^{a-1} f_i(x) i y^{i-1} \right) y^l \, dy
\]

(\ast)

- Partially integrating the right-hand side to \( y \) gives

\[
d \left( x^j \left( \frac{a}{a+l} y^{a+l} + \sum_{i=1}^{a-1} \frac{i}{i+l} f_i(x) y^{i+l} \right) \right) \equiv 0
\]

- This gives an expression for the right-hand side of (\ast) and thus

\[
x^j \left( \sum_{i=1}^{a-1} \frac{l}{i+l} f_i'(x) y^i + f_0'(x) \right) y^l \, dx \equiv j x^{j-1} \left( \frac{a}{a+l} y^{a} + \sum_{i=1}^{a-1} \frac{i}{i+l} f_i(x) y^i \right) y^l \, dx
\]
The action of $\sigma_*$ on a differential form $x^k y^l dx$ is given by

$$\sigma_*(x^k y^l dx) \equiv (x^\sigma)^k (y^\sigma)^l \, dx^\sigma.$$  

Substituting power series for $x^\sigma$ and $y^\sigma$, we can write $\sigma_*(x^k y^l dx)$ on basis of $H^1(\overline{A}/\mathbb{Q}_q)$ using the reduction formulae.

This gives matrix $M$ which is an approximation of the action of $\sigma_*$ on $H^1(\overline{A}/\mathbb{Q}_q)$.

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

Complexity: $O(g^{5+\varepsilon} n^{3+\varepsilon})$ time and $O(g^3 n^3)$ space.
# Experimental Results

Genus 2 curves over $\mathbb{F}_{2^n}$  

<table>
<thead>
<tr>
<th>$n$</th>
<th>Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>18.1</td>
</tr>
<tr>
<td>72</td>
<td>36.5</td>
</tr>
<tr>
<td>84</td>
<td>52.8</td>
</tr>
<tr>
<td>96</td>
<td>88.8</td>
</tr>
<tr>
<td>120</td>
<td>238</td>
</tr>
<tr>
<td>144</td>
<td>437</td>
</tr>
<tr>
<td>168</td>
<td>757</td>
</tr>
<tr>
<td>192</td>
<td>1229</td>
</tr>
<tr>
<td>240</td>
<td>3760</td>
</tr>
</tbody>
</table>

Genus $g$ hyp. curves over $\mathbb{F}_2$  

<table>
<thead>
<tr>
<th>Genus</th>
<th>Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>13.3</td>
</tr>
<tr>
<td>40</td>
<td>116</td>
</tr>
<tr>
<td>60</td>
<td>458</td>
</tr>
<tr>
<td>80</td>
<td>897</td>
</tr>
<tr>
<td>100</td>
<td>2118</td>
</tr>
<tr>
<td>120</td>
<td>4593</td>
</tr>
<tr>
<td>160</td>
<td>11759</td>
</tr>
<tr>
<td>200</td>
<td>33531</td>
</tr>
<tr>
<td>240</td>
<td>39120</td>
</tr>
</tbody>
</table>
## Experimental Results

<table>
<thead>
<tr>
<th>$gn$</th>
<th>$C_{3,4}$ curves</th>
<th>$C_{3,5}$ curves</th>
</tr>
</thead>
<tbody>
<tr>
<td>120</td>
<td>1360</td>
<td>2440</td>
</tr>
<tr>
<td>144</td>
<td>4073</td>
<td>4926</td>
</tr>
<tr>
<td>168</td>
<td>4978</td>
<td>7094</td>
</tr>
<tr>
<td>192</td>
<td>7297</td>
<td>12093</td>
</tr>
<tr>
<td>240</td>
<td>15909</td>
<td>27078</td>
</tr>
<tr>
<td>288</td>
<td>30044</td>
<td>44786</td>
</tr>
</tbody>
</table>
Conclusions & Open Problems

• Now possible to compute the zeta function of hyperelliptic curves and \( C_{a,b} \) curves over finite fields of any small characteristic.

• Complexity: \( O(g^{5+\varepsilon}n^{3+\varepsilon}) \) operations and \( O(g^3n^3) \) space.

• Lifting works for arbitrary non-singular affine curves, but how easy is it to write down explicit basis and reduction formulae?
  – WIP: Riemann-Roch theorem to construct differentials.

• Need new ideas for practical algorithms to deal with large \( p \)!