Counting Points on Hyperelliptic Curves over Finite Fields of Small Characteristic

Frederik Vercauteren

Computer Science Department

University of Bristol

Woodland Road, Bristol BS8 1UB, United Kingdom

frederik@cs.bris.ac.uk

Overview

- Hyperelliptic curves
- Zeta functions and Weil conjectures
- Monsky-Washnitzer cohomology
- Kedlaya's algorithm for odd characteristic
- Extending Kedlaya's algorithm to characteristic 2

Hyperelliptic Curves

Hyperelliptic curve $\overline{C}$ of genus g over finite field $\mathbb{F}_q$,

$$\overline{C} : y^2 + \overline{h}(x)y = \overline{f}(x)$$

where $\deg \overline{h} \leq g$, $\overline{f}$ monic, $\deg \overline{f} = 2g + 1$ and $\overline{C}$ non-singular.

If char $\mathbb{F}_q > 2$ one can take $\overline{h} = 0$ and $\overline{f}$ has to be squarefree.

Jacobian $\mathrm{Jac}(\overline{C}/\mathbb{F}_q)$ is abelian group associated with $\overline{C}$ which is quotient group of degree 0 divisors by principal divisors.

Problem: compute order of $\mathrm{Jac}(\overline{C}/\mathbb{F}_q)$.

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 $a_{g+i} = q^i a_{g-i}$
- $N_r = q^r + 1 - \sum_{i=0}^{2g} \alpha_i^r$ and $P(1)$ is the order of $\mathrm{Jac}(\overline{C}/\mathbb{F}_q)$

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 K can be constructed as

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

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

- Galois group of K over $\mathbb{Q}_p$ is cyclic with generator Frobenius substitution σ and σ modulo M_R equals small Frobenius on $\mathbb{F}_q$.

Computing Zeta Function - General Strategy

- $\overline{X}$ smooth affine variety over $\mathbb{F}_q$ of dimension n
- Monsky and Washnitzer construct vectorspaces $H^i(\overline{X}/K)$ over K with an induced action of Frobenius F_* on it such that

$$N_r = \sum_{i=0}^{n} (-1)^i \mathrm{Tr}\left((q^n F_*^{-1})^r | H^i(\overline{X}/K)\right)$$

$$Z(\overline{X};t) = \prod_{i \text{ odd}} P_i(t) \prod_{i \text{ even}} P_i(t)^{-1},$$

with $P_i(t) = \det(1 - tq^n F_*^{-1} | H^i(\overline{X}/K))$.

Monsky-Washnitzer Cohomology

- $\overline{X}$ smooth affine variety over $\mathbb{F}_q$ with coordinate ring $\overline{A}$
- Let A be finitely generated R-algebra with $A/pA \cong \overline{A}$
- One would like to have lift of Frobenius endomorphism on A, but in general this is not possible.
- Working with p-adic completion A^∞ of A does admit a lift, but the de Rham cohomology of A^∞ can be larger than the one 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. Work with subalgebra $A^\dagger$ satisfying certain growth conditions.

Dagger rings

- Dagger ring $A^\dagger$ of $A := R[x_1, \dots, x_n]/(f_1, \dots, f_m)$ is

$$A^\dagger := R\langle x_1, \dots, x_n\rangle^\dagger/(f_1, \dots, f_m),$$

where $R\langle x_1, \dots, x_n\rangle^\dagger$ consists of power series

$$\left\{\sum a_\alpha x^\alpha \in R[[x_1, \dots, x_n]] \mid \exists C, \rho \in \mathbb{R}, C > 0, 0 < \rho < 1, \forall \alpha : |a_\alpha| \leq C\rho^{|\alpha|}\right\},$$

where $\alpha := (\alpha_1, \dots, \alpha_n)$, $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and $|\alpha| := \sum_{i=0}^n \alpha_i$.

- Let $\overline{B}/k$ be finitely generated, with lift $B^\dagger$ and $g : \overline{A} \to \overline{B}$ be a morphism of k-algebra's, then there exists an R-homomorphism $G : A^\dagger \to B^\dagger$ lifting g.

Monsky-Washnitzer Cohomology Groups

- Define universal module $D^1(A^\dagger)$ of differentials

$$D^1(A^\dagger) := (A^\dagger\ dx_1 + \cdots + A^\dagger\ dx_n)/(\sum_{i=1}^{m} A^\dagger(\frac{\partial f_i}{\partial x_1}\ dx_1 + \cdots + \frac{\partial f_i}{\partial x_n}\ dx_n)).$$

- Let $D^i(A^\dagger) := \bigwedge^i D^1(A^\dagger)$ the i-th exterior product of $D^1(A^\dagger)$ and $d_i : D^i(A^\dagger) \to D^{i+1}(A^\dagger)$ the exterior differentiation. Since $d_{i+1} \circ d_i = 0$ we get the de Rham complex $D(A^\dagger)$

$$0 \longrightarrow D^0(A^\dagger) \xrightarrow{d_0} D^1(A^\dagger) \xrightarrow{d_1} D^2(A^\dagger) \xrightarrow{d_2} D^3(A^\dagger) \cdots.$$

- Define i-th cohomology group $H^i(\overline{A}/R) := \mathrm{Ker}\ d_i/\mathrm{Im}\ d_{i-1}$ and $H^i(\overline{A}/K) := H^i(\overline{A}/R) \otimes_R K$ gives i-th Monsky-Washnitzer cohomology group.

Kedlaya's Algorithm

- Let $y^2 - \overline{f}(x) = 0$ hyperelliptic curve $\overline{C}$ of genus g over $\mathbb{F}_{p^n}$ with p small, odd prime.
- Affine curve $\overline{C}'$ obtained from C by deleting support of divisor of y, then coordinate ring $\overline{A}$ of $\overline{C}'$ is $\mathbb{F}_q[x, y, y^{-1}]/(y^2 - \overline{f}(x))$.
- Lift $\overline{C}'$ to C' over R by taking any lift $f(x) \in R[x]$ of $\overline{f}(x)$ and removing point at infinity and Weierstrass points of the affine curve curve $y^2 - f(x) = 0$.
- The coordinate ring of C' then is $A = R[x, y, y^{-1}]/(y^2 - f(x))$.
- The elements of the dagger ring $A^\dagger$ can be viewed as 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 $|k|$.

Kedlaya's Algorithm

- For a smooth affine curve $\overline{C}'$ one has $H^i(\overline{A}/K) = 0$ for $i > 1$.
- Only need to look at $H^0(\overline{A}/K)$ and $H^1(\overline{A}/K)$:
  - From the definition we see that $H^0(\overline{A}/K) = K$
  - Kedlaya proves that $H^1(\overline{A}/K) = H^1(\overline{A}/K)^+ \oplus H^1(\overline{A}/K)^-$
    - $H^1(\overline{A}/K)^+$ is invariant under involution and generated by $x^i dx/y^2$ for $i = 0, \ldots, 2g$
    - $H^1(\overline{A}/K)^-$ is anti-invariant under involution and 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 $H^1(\overline{A}/K)^-$ equals $\chi(t) := t^{2g}P(1/t)$ with $Z(\overline{C};t) = \frac{P(t)}{(1-t)(1-qt)}$.

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 $A^\dagger$:

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

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 in Characteristic 2 - First Attempt

- Let $\overline{C}$ be hyperelliptic curve over $\mathbb{F}_{2^n}$ given by the equation

$$\overline{C} : y^2 + \overline{h}(x)y = \overline{f}(x).$$

- Consider $\overline{C}'$ obtained from $\overline{C}$ by removing the support of the divisor of $2y + \overline{h}(x)$, then the coordinate ring of $\overline{C}'$ is

$$\overline{A} = \mathbb{F}_{2^n}[x, y, (2y + \overline{h}(x))^{-1}]/(y^2 + \overline{h}(x)y - \overline{f}(x)).$$

- Take any lift $C : y^2 + h(x)y - f(x) = 0$ of $\overline{C}$ over R and consider the curve C' obtained from C by removing the support of divisor of $2y + h(x)$, then C' has coordinate ring

$$A = R[x, y, (2y + h(x))^{-1}]/(y^2 + h(x)y - f(x)).$$

Kedlaya in Characteristic 2 - First Attempt

- Write the curve C as $(2y + h(x))^2 = 4f(x) + h(x)^2$, then we are in a similar situation as Kedlaya's original algorithm.

- Lifting σ to $A^\dagger$ as $x^\sigma = x^2$ and $(2y + h(x))^\sigma$ defined by $((2y + h(x))^\sigma)^2 = 4f(x)^\sigma + (h(x)^\sigma)^2$ gives problems, since during Newton iteration one has to reduce modulo $4f(x) + h(x)^2$.

- The dimension of $H^1(\overline{A}/K)$ is determined by the number of points one removes from $\overline{C}$. Kedlaya finds a basis for $H^1(\overline{A}/K)$ by constructing a basis for the de Rham cohomology of A and proving that this also gives a basis for $H^1(\overline{A}/K)$.

- The dimension of the de Rham cohomology is determined by the number of points you remove from C.

Kedlaya in Characteristic 2 - Isomorphic Curve

- Given the hyperelliptic curve $\overline{C} : y^2 + \overline{h}(x)y = \overline{f}(x)$, let $\overline{\theta}_i \in \overline{\mathbb{F}}_q$ for $i = 1, \ldots, s$ be the different zeros of $\overline{h}(x)$.
- Define the polynomial $\overline{H}(x) = \prod_{i=0}^{s}(x - \overline{\theta}_i) \in \mathbb{F}_q[x]$.
- We can assume that $\overline{H}(x) \mid \overline{f}(x)$, since the isomorphism defined by $x \mapsto x$ and $y \mapsto y + \sum_{i=0}^{s} b_i x^i$ transforms the curve in

$$y^2 + h(x)y = f(x) - \sum_{i=0}^{s} b_i^2 x^{2i} - h(x) \sum_{i=0}^{s} b_i x^i.$$

- Sufficient to choose $b_i \in \mathbb{F}_q$ such that $f(\overline{\theta}_j) = \sum_{i=0}^{s} b_i^2 \cdot \overline{\theta}_j^{2i}$ for $j = 0, \ldots, s$.

Kedlaya in Characteristic 2 - Lift of Curve

- Consider the curve $\overline{C}'$ by removing the point at infinity and the s points $(\bar{\theta}_i, 0)$ for $i = 1, \ldots, s$. The coordinate ring $\overline{A}$ of C' is

$$\mathbb{F}_{2^n}[x, y, \overline{H}(x)^{-1}]/(y^2 + \bar{h}(x)y - \bar{f}(x)).$$

- Take any lift $H(x) \in R[x]$ of $\overline{H}(x)$ and lift $\bar{h}(x)$ and $\bar{f}(x)$ in such a way that $H(x)|h(x)$ and $H(x)|f(x)$.

- Consider the curve C' obtained from $C : y^2 + h(x)y - f(x) = 0$ by removing the point at infinity and the s points $(\theta_i, 0)$ with $H(\theta_i) = 0$ for $i = 1, \ldots, s$. Then the coordinate ring A of C' is

$$R[x, y, H(x)^{-1}]/(y^2 + h(x)y - f(x)).$$

Kedlaya in Characteristic 2 - Dagger Ring

- Let $A^\dagger$ be the dagger ring of A. Any element of $A^\dagger$ can be written as a series $\sum_{k=-\infty}^{\infty}(S_k(x)+T_k(x)y)H(x)^k$, with $\deg S_k, \deg T_k \leq \deg H$.
- The growth condition on the dagger ring implies that the valuation of S_k, T_k grows linearly with $|k|$.
- Lift $\overline{\sigma}$ to an endomorphism σ of $A^\dagger$ by defining it as $x^\sigma = x^2$ and y^σ by $(y^\sigma)^2 + h(x)^\sigma y^\sigma - f(x)^\sigma = 0$.
- An approximation for y^σ is computed as a Laurent series $\sum_{i=-L}^{L}(S_i(x)+T_i(x)y)H(x)^i$ via the Newton iteration

$$W_{k+1} = W_k - \frac{W_k^2 + h(x)^\sigma W_k - f(x)^\sigma}{2W_k + h(x)^\sigma} \bmod 2^{k+1}.$$

Kedlaya in Characteristic 2 - $H^1(\overline{A}/K)$

- The de Rham cohomology of A splits under involution:
  - invariant part generated by $x^i/H(x)\,dx$ for $0 \leq i < \deg H$
  - anti-invariant part generated by $x^i y\,dx$ for $0 \leq i < 2g$
- Analogous to Kedlaya, we devise reduction formulae to express any differential form on this basis.
- The reduction of $T_k(x)H(x)^k y\,dx$ becomes integral upon multiplication with $c = 3 + \lfloor \log_2(|k+1| \cdot \deg H + g + 1) \rfloor$.
- Basis for the de Rham cohomology of A is basis for $H^1(\overline{A}/K)$.

Kedlaya in Characteristic 2 - Zeta Function

- Again it is sufficient to compute the action of Frobenius F_* on $H^1(\overline{A}/K)^-$ to recover the characteristic polynomial $\chi(t)$.
- The action of σ_* on a differential form $x^k y dx$ is given by

$$\sigma_*(x^k y dx) \equiv 2x^{2k+1} y^\sigma dx.$$

- Substituting the approximation for y^σ, we can write $\sigma_*(x^k y dx)$ on the basis of $H^1(\overline{A}/K)^-$ using the reduction formulae.
- 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 $M M^\sigma \cdots M^{\sigma^{n-1}}$.

Conclusions

- Now possible to compute the zeta function of hyperelliptic curve over finite field of any small characteristic.
- Complexity: $O(g^{5+\varepsilon}n^{3+\varepsilon})$ operations and $O(g^3n^3)$ space.
- Resulting algorithms can be used to generate hyperelliptic curves suitable for cryptography, but not as fast as AGM.
- Can we get rid of cubic space complexity ?
- How easy is the algorithm to write down for more general curves or even surfaces ?