

EXTENSIONS OF KEDLAYA'S ALGORITHM

Frederik Vercauteren

frederik@cs.bris.ac.uk

—

Jan Denef

jan.denef@wis.kuleuven.ac.be



University of Leuven



<http://www.arihcc.com>



University of Bristol

Overview

- “Who’s who” of p -adic point counting
- Zeta functions and Weil conjectures
- Monsky-Washnitzer cohomology
- Kedlaya’s algorithm for hyperelliptic curves in characteristic 2
- Kedlaya’s algorithm for $C_{a,b}$ curves
- Experimental results
- Conclusions and open problems

“Who’s who” of p -adic point counting

Elliptic Curves over \mathbb{F}_{p^n}	p	Time	Space
Satoh	$p \geq 5$	$O(n^{3+\epsilon})$	$O(n^3)$
Skjernaa	$p = 2$	$O(n^{3+\epsilon})$	$O(n^3)$
Fouquet-Gaudry-Harley	$p = 2, 3$	$O(n^{3+\epsilon})$	$O(n^3)$
Vercauteren	all p	$O(n^{3+\epsilon})$	$O(n^2)$
Mestre-Harley (AGM)	$p = 2$	$O(n^{3+\epsilon})$	$O(n^2)$
Satoh-Skjernaa-Taguchi	all p	$O(n^{2+1/2+\epsilon})$	$O(n^2)$
Gaudry	$p = 2$	$O(n^{2+1/2+\epsilon})$	$O(n^2)$
Carls	all p	$O(n^{3+\epsilon})$	$O(n^2)$
Harley	all p	$O(n^{2+1/2+\epsilon})$	$O(n^2)$

“Who’s who” of p -adic point counting

Hyperelliptic curves over \mathbb{F}_{p^n}	p	Time	Space	Genus
Kedlaya	$p \geq 3$	$O(g^{4+\varepsilon}n^{3+\varepsilon})$	$O(g^3n^3)$	all g
Mestre-Gaudry-Harley	$p = 2$	$O(n^{3+\varepsilon})$	$O(n^2)$	$g = 2$ (O)
Lauder-Wan	all p	$O(g^{5+\varepsilon}n^{3+\varepsilon})$	$O(g^3n^3)$	all g (AS)
Denef-Vercauteren	$p = 2$	$O(g^{4+\varepsilon}n^{3+\varepsilon})$	$O(g^3n^3)$	all g
Mestre-Lercier-Lubicz	$p = 2$	$O(n^{3+\varepsilon})$	$O(n^2)$	$g = 2$ (O)

Superelliptic curves over \mathbb{F}_{p^n}	p	Time	Space	Genus
Gaudry-Gürel	all p	$O(g^{4+\varepsilon}n^{3+\varepsilon})$	$O(g^3n^3)$	all g
Lauder	all p	$O(g^{4+\varepsilon}n^{3+\varepsilon})$	$O(g^3n^3)$	$a p - 1$

$C_{a,b}$ curves over \mathbb{F}_{p^n}	p	Time	Space	Genus
Denef-Vercauteren	all p	$O(g^{2+\varepsilon}n^{3+\varepsilon})$	$O(g^2n^3)$	all g
Algebraic varieties over \mathbb{F}_{p^n}	p	Time	Space	
Lauder-Wan	all p	Polynomial	Polynomial	

The Zeta Function and Weil Conjectures

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

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

with N_r the number of points on \tilde{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 \tilde{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 $\text{Jac}(\tilde{C}/\mathbb{F}_q)$

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

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

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

$$\#\overline{C}(\mathbb{F}_{q^r}) = q^r - \text{Trace} \left((q F_*^{-1})^r | H^1(\overline{C}/K) \right)$$

Hyperelliptic Curves

- **Hyperelliptic curve** \bar{C} of genus g over finite field \mathbb{F}_q ,

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

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

- If $\text{char } \mathbb{F}_q > 2$ one can take $\bar{h} = 0$ and \bar{f} has to be squarefree.
- **Jacobian** $\text{Jac}(\bar{C}/\mathbb{F}_q)$ is abelian group associated with \bar{C} which is quotient group of degree 0 divisors by principal divisors.
- **Problem:** compute order of $\text{Jac}(\bar{C}/\mathbb{F}_q)$.

Kedlaya in Characteristic 2 - Isomorphic Curve

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

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

- Compute $b_i \in \mathbb{F}_q$ such that $f(\bar{\theta}_j) = \sum_{i=0}^s b_i^2 \cdot \bar{\theta}_j^{2i}$ for $j = 0, \dots, s$.
- **Note:** $(\bar{\theta}_i, 0) \in \bar{C}$ for $i = 0, \dots, s$ are invariant under involution.

Kedlaya in Characteristic 2 - Lift of Curve

- \overline{C}' is \overline{C} minus the points $(\overline{\theta}_i, 0)$ for $0 \leq i \leq s$ with coordinate ring

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

- Take any lift $H(x) \in R[x]$ of $\overline{H}(x)$ and lift $\overline{h}(x)$ and $\overline{f}(x)$ in such a way that $H(x)|h(x)$ and $H(x)|f(x)$.
- C' is $C : y^2 + h(x)y - f(x) = 0$ minus the points $(\theta_i, 0)$ with $H(\theta_i) = 0$ for $0 \leq i \leq s$ with coordinate ring

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

- **Note:** if $H(x) \nmid f(x)$ then $(\overline{\theta}_i, \sqrt{f(\overline{\theta}_i)})$ splits into 2 points $(\theta_i, \pm \sqrt{f(\theta_i)})$ and so $\dim H_{DR}^1(A/K) \neq \dim H^1(\overline{A}/K)$.

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 $\bar{\sigma}$ to an endomorphism σ of A^\dagger by defining it as
 - Frobenius substitution σ on R
 - $x^\sigma = x^2$
 - y^σ by $(y^\sigma)^2 + h(x)^\sigma y^\sigma - f(x)^\sigma = 0$ and $y^\sigma \equiv y^2 \pmod{2}$.

Kedlaya in Characteristic 2 - Frobenius on A^\dagger

- An approximation for y^σ is computed as a Laurent series $\sum_{i=-L_k}^{A_k} (S_i(x) + T_i(x)y)H(x)^i$ via the Newton iteration

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

- We can prove tight bounds on the convergence of W_k by

$$\begin{aligned} A_k &\leq 2k \frac{(\deg f - 2 \deg h)}{\deg H} + 2 \frac{\deg h}{\deg H}, \\ L_k &\leq 4kD - 2D, \end{aligned}$$

with D the max multiplicity of the irreducible factors of $\bar{h}(x)$.

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

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

$$D^1(A^\dagger) := (A^\dagger dx + A^\dagger dy) / ((2y + h(x)) dy + (h'(x)y - f'(x)) dx)$$

- Let $d : A^\dagger \rightarrow D^1(A^\dagger)$ be differentiation, then

$$H^1(\bar{A}/K) := D^1(A^\dagger) / d(A^\dagger) \otimes_R K$$

- A differential of the form $d(\alpha)$ with $\alpha \in A^\dagger$ is called **exact**.
- $H^1(\bar{A}/K)$ is vector space over K of **dimension** $2g + m - 1$, where m is the # points needed to complete \bar{C}' to a projective curve.

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

- $H^1(\bar{A}/K)$ splits into eigenspaces under involution:
 - invariant part H_+^1 with basis $x^i/H(x) dx$ for $0 \leq i < \deg H$
 - anti-invariant part H_-^1 with basis $x^i y dx$ for $0 \leq i < 2g$
- **Note:** the invariant part H_+^1 corresponds to the removed points $(\bar{\theta}_i, 0)$ for $i = 0, \dots, s$, with $s + 1 = \dim H_+^1$.
- Analogous to Kedlaya, we devise reduction formulae to express any differential form on this basis.

Kedlaya in Characteristic 2 - Trace Formula

- The Frobenius σ on A^\dagger induces an **action** σ_* on $H^1(\bar{A}/K)$ by pullback, i.e. $\sigma_*(d\alpha) = d(\alpha^\sigma)$ with $\alpha \in A^\dagger$.
- The **n -fold composite** $F_* = \sigma_*^n$ defines a K -linear map on $H^1(\bar{A}/K)$ which commutes with the hyperelliptic involution.
- A consequence of the Lefschetz trace formula is

$$\#\tilde{C}(\mathbb{F}_{q^r}) = q^r + 1 - \text{Trace}(F_*^r, H_-^1)$$

- The characteristic polynomial $\chi(t)$ of F_* on H_-^1 determines the zeta function of \tilde{C} as

$$Z(\tilde{C}; t) = \frac{t^{2g} \chi(1/t)}{(1-t)(1-qt)}$$

Kedlaya in Characteristic 2 - Zeta Function

- 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 $MM^\sigma \cdots M^{\sigma^{n-1}}$.

Kedlaya's Algorithm - Complexity

Complexity for genus g hyperelliptic curve over \mathbb{F}_{p^n}

Algorithm	Time Complexity	Space Complexity
Char $p \neq 2$: Kedlaya	$O(g^{4+\varepsilon} n^{3+\varepsilon})$	$O(g^3 n^3)$
Char 2 : Average case	$O(g^{4+\varepsilon} n^{3+\varepsilon})$	$O(g^3 n^3)$
Char 2 : Worst case	$O(g^{5+\varepsilon} n^{3+\varepsilon})$	$O(g^4 n^3)$

- Complexity depends on splitting type of $\bar{h}(x) = \prod_{i=1}^s (x - \bar{\theta}_i)^{m_i}$.
- Worst case is $s \approx g/2$, $m_i = 1$ for $0 < i < s$ and $m_s \approx g/2$.

$C_{a,b}$ curves

- $C_{a,b}$ curve \bar{C} over finite field \mathbb{F}_q ,

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

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

- Absolutely irreducible and if smooth 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: $\bar{f}_i(x) = 0$ for $i = 1, \dots, a - 1$

$C_{a,b}$ curves - Lift of Curve

- The affine curve \overline{C} has coordinate ring $\overline{A} := \mathbb{F}_q[x, y]/(\overline{C})$.
- Take arbitrary lifts $f_i(x) \in R[x]$ of $\overline{f}_i(x)$ for $i = 0, \dots, a - 1$ 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 $A := R[x, y]/(C)$.
- Elements of A^\dagger can be represented as $\sum_{l=0}^{a-1} \sum_{k=0}^{+\infty} a_{k,l} x^k y^l$ 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 σ on A^\dagger are

$$x^\sigma \equiv x^p \pmod{p} \quad \text{and} \quad y^\sigma \equiv y^p \pmod{p} \quad \text{and} \quad C^\sigma(x^\sigma, y^\sigma) = 0$$

- **Fixing** $x^\sigma = x^p$ also fixes y^σ 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

$$C^\sigma(x^\sigma, y^\sigma) = C^\sigma(x^p + \alpha Z, y^p + \beta Z) = 0 \quad \text{and} \quad Z \equiv 0 \pmod{p}$$

$C_{a,b}$ curves - Frobenius on A^\dagger

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

$$G'(Z) \equiv \alpha \frac{\partial C^\sigma}{\partial x} \Big|_{(x^p, y^p)} + \beta \frac{\partial C^\sigma}{\partial y} \Big|_{(x^p, y^p)} + O(Z) \pmod{p}$$

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

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

- 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 $H^1(\bar{A}/K)$

- If \bar{C} is smooth, then $2g = (a-1)(b-1)$ and a basis for $H^1(\bar{A}/K)$
 $x^k y^l dx$ for $k=0, \dots, b-2$ and $l=1, \dots, a-1$
- 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

$$\sum_{i=1}^{a-1} f'_i(x) y^i + f'_0(x) dx = -\sum_{i=1}^{a-1} f_i(x) i y^{i-1} dy$$

$C_{a,b}$ curves - Reduction Formula

- To reduce $x^i y^l dx$ we multiply this equation with $x^j y^l$

$$x^j \left(\sum_{i=1}^{a-1} f'_i(x) y^i + f'_0(x) \right) y^l dx = -x^j (a y^{a-1} + \sum_{i=1}^{a-1} f_i(x) i y^{i-1}) y^l dy \quad (*)$$

- 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 (*) and thus

$$x^j \left(\sum_{i=1}^{a-1} \frac{l}{i+l} f'_i(x) y^i + f'_0(x) \right) y^l dx \equiv j x^{j-1} \left(\frac{a}{a+l} y^a + \sum_{i=1}^{a-1} \frac{i}{i+l} f_i(x) y^i \right) y^l dx$$

$C_{a,b}$ -curves - Zeta Function

- The action of σ_* 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^σ and y^σ , we can write $\sigma_*(x^k y^l dx)$ on basis of $H^1(\bar{A}/K)$ using the reduction formulae.
- This gives matrix M which is an approximation of the action of σ_* on $H^1(\bar{A}/K)$.
- The polynomial $\chi(t) := t^{2g} P(1/t)$ can then be approximated by the characteristic polynomial of $MM^\sigma \cdots M^{\sigma^{n-1}}$.

Dependence on size of Jacobian

Timings for **180-bit Jacobians** of hyperelliptic curves for various genus g and extension degrees n .

Genus g	Degree n	Lifting y^σ (s)	Reduction (s)	Total (s)
2	90	69.6	29.5	101
3	60	83.4	35.2	120
4	45	87.2	45.3	135
5	36	96.7	50.5	151
10	18	217	149	369
15	12	254	232	489
20	9	385	376	765

Kedlaya in Char 2 - Example: Genus 3 over $\mathbb{F}_{2^{59}}$

Let $\mathbb{F}_{2^{59}}$ be defined as $\mathbb{F}_2[t]/\overline{P}(t)$ with $\overline{P}(t) = t^{59} + t^7 + t^4 + t^2 + 1$ and consider the random hyperelliptic curve C_3 of genus 3 defined by

$$y^2 + \left(\sum_{i=0}^3 h_i x^i \right) y = x^7 + \sum_{i=0}^6 f_i x^i,$$

where

$h_0 =$	$h_1 =$	$h_2 =$	$h_3 =$
569121E97EB3821	49F340F25EA38A2	2DE854D48D56154	0B6372FF7310443
$f_0 =$	$f_1 =$	$f_2 =$	$f_3 =$
1104FDBEB454C58	0C426890E5C7481	34967E2EB7D50C3	1F1728AA28C616C
$f_4 =$	$f_5 =$	$f_6 =$	
1AE177BFFE49826A	3895A0E400F7D18	6DF634A1E2BFA8E	

The group order of the Jacobian $J_{\tilde{C}_3}$ of C_3 over $\mathbb{F}_{2^{59}}$ is

$$\#J_{\tilde{C}_3} = 2 \cdot 957809714072433946337623323601231603334059170481903949$$

where the last factor is 176-bit prime.

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: $O(g^{4+\varepsilon}n^{3+\varepsilon})$ operations and $O(g^3n^3)$ space.
- Resulting algorithms can be used to **generate curves suitable for cryptography**, but not as fast as AGM.
- Can we get substantial improvement for **ordinary curves** ?
- Lifting works for arbitrary **non-singular affine curves**, but how easy is it to write down **explicit basis** and **reduction formulae** ?
- **Golden grail**: practical algorithms for **large p** ?