Fast arithmetics for Artin-Schreier extensions

L. De Feo
joint work with Éric Schost

École Polytechnique, Paris, France

February 27, 2009
LIP6, Séminaire Salsa, Paris

Artin-Schreier

Definition (Artin-Schreier polynomial)

$\mathbb{K}$ a field of characteristic p, $\alpha \in \mathbb{K}$

$$X^p - X - \alpha$$

is an Artin-Schreier polynomial.

Theorem

$\mathbb{K}$ *finite.* $X^p - X - \alpha$ *irreducible* $\Leftrightarrow$ $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}_p}(\alpha) \neq 0$.
If $\eta \in \mathbb{K}$ *is a root, then* $\eta + 1, \ldots, \eta + (p-1)$ *are roots.*

Definition (Artin-Schreier extension)

$\mathcal{P}$ an irreducible Artin-Schreier polynomial.

$$\mathbb{L} = \mathbb{K}[X]/\mathcal{P}(X).$$

$\mathbb{L}/\mathbb{K}$ is called an Artin-Schreier extension.

Our context

$$\mathbb{U}_k = \frac{\mathbb{U}_{k-1}[X_k]}{P_{k-1}(X_k)}$$

$$\Big|\, p$$

$$\mathbb{U}_{k-1}$$

$$\vdots$$

$$\mathbb{U}_1 = \frac{\mathbb{U}_0[X_1]}{P_0(X_1)}$$

$$\Big|\, p$$

$$\mathbb{U}_0 = \mathbb{F}_{p^d} = \frac{\mathbb{F}_p[X_0]}{Q(X_0)}$$

Towers over finite fields

$$P_i = X^p - X - \alpha_i$$

We say that $(\mathbb{U}_0, \ldots, \mathbb{U}_k)$ is defined by $(\alpha_0, \ldots, \alpha_{k-1})$ over $\mathbb{U}_0$.

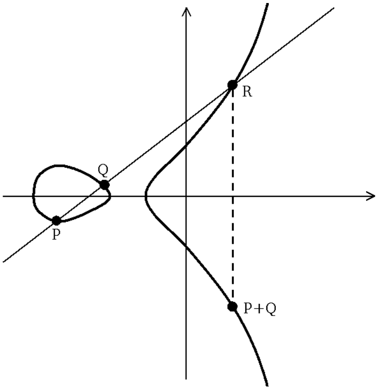
ANY extension of degree p can be expressed this way

Motivations

- p-torsion points of abelian varieties;
- Isogeny computation [Couveignes '96].

Elliptic curves over finite fields

$$\mathbf{E} \ : \ Y^2 = X^3 + aX + b$$



$$a, b \in \mathbb{F}_q = \mathbb{F}_{p^d} \qquad p \neq 2, 3$$

$\mathcal{O}$, the point at infinity, is the zero of the law

Elliptic curves - Multiplication

$$[m]P = \underbrace{P + P + \cdots + P}_{m \text{ times}}$$

Multiplication

$$[m]P = \left(\frac{\phi_m(X,Y)}{\psi_m^2(X,Y)}, \frac{\omega_m(X,Y)}{\psi_m^3(X,Y)} \right)$$

with $\deg \psi^2 \approx \deg \phi \approx m^2$, $\qquad \psi_m(X_P, Y_P) = 0 \Leftrightarrow [m]P = \mathcal{O}$.

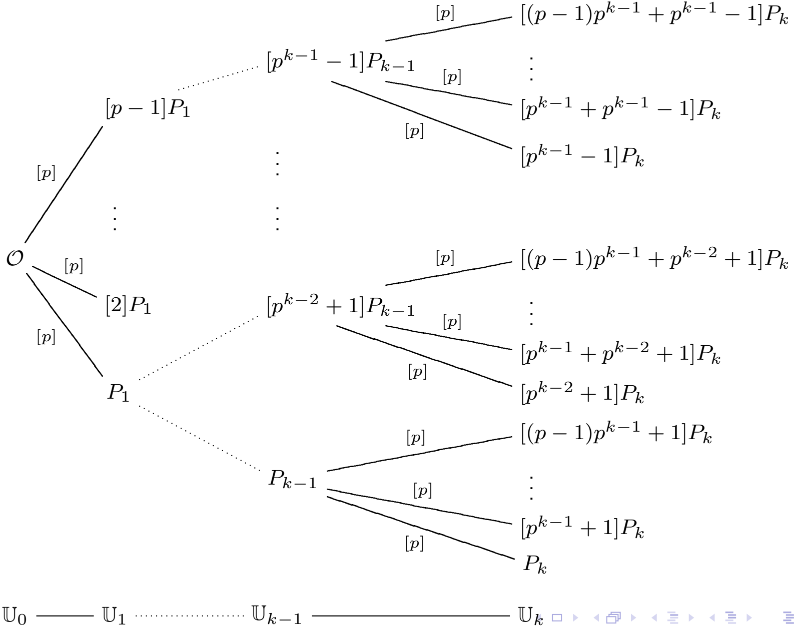
Torsion group

$$E[m] = \left\{ P \in E(\bar{\mathbb{F}}_q) \;\middle|\; [m]P = \mathcal{O} \right\}$$

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \quad \text{if } m \text{ prime to } p$$

$$E[p^k] \cong \begin{cases} \mathbb{Z}/p^k\mathbb{Z} & \textit{ordinary} \text{ case} \\ \{\mathcal{O}\} & \textit{supersingular} \text{ case} \end{cases}$$

Structure of the p^k-torsion



Structure of the p^k-torsion

p^k-torsion

- $E[p^i]$ not necessarily defined over $\mathbb{F}_q$,
- if $E[p^i]$ defined over $\mathbb{K}$, then $E[p^{i+1}]$ defined over $\mathbb{K}[X]/\psi_p(X)$,
- $\psi_p(X) = V(X)^p$ with V separable of degree p.

Theorem

Let $(\mathbb{K} = \mathbb{U}_0, \ldots, \mathbb{U}_k)$ *be the tower of minimal degree s.t.* $E[p^i] \subset E(\mathbb{U}_i)$ *for any* i. *Then there is a* i_0 *s.t.* $\mathbb{U}_{i_0} = \mathbb{U}_0$ *and for* $i \geqslant i_0$

$$[\mathbb{U}_{i+1} : \mathbb{U}_i] = p,$$

Going further

- Generalizes to higher genus curves: $C[p^k] = \left(\mathbb{Z}/p^k\mathbb{Z}\right)^g$.
- Applications to point counting: interpolate rational maps over the p^k-torsion points.

Size, complexities

$$\#\mathbb{U}_i = p^{p^i d}$$

$\mathbb{U}_k$ — $\mathbb{U}_{k-1}$ - - - $\mathbb{U}_1$ — $\mathbb{U}_0$

Optimal representation

All common representations achieve it: $O(p^i d \log p)$

Complexities in $\mathbb{F}_p$-operations

optimal:	$O(p^i d)$	addition
quasi-optimal:	$\tilde{O}(i^a p^i d)$	FFT multiplication
almost-optimal:	$\tilde{O}(i^a p^{i+b} d)$	
suboptimal:	$\tilde{O}(i^a p^{i+b} d^c)$	
too bad:	$\tilde{O}\left(i^a (p^{i+b})^e d^c\right)$	naive multiplication

Multiplication function $\mathsf{M}(n)$

FFT: $\mathsf{M}(n) = O(n \log n \log\log n)$, Naive: $\mathsf{M}(n) = O(n^2)$.

Representation matters!

$\mathbb{U}_k$

$\mathbb{U}_{k-1}$

$\mathbb{U}_1$

$\mathbb{U}_0$

Multivariate representation of $v \in \mathbb{U}_i$

$$v = X_0^{d-1} X_1^{p-1} \cdots X_i^{p-1} + 2X_0^{d-1} X_1^{p-1} \cdots X_i^{p-2} + \cdots$$

Univariate representation of $v \in \mathbb{U}_i$

- $\mathbb{U}_i = \mathbb{F}_p[x_i]$,
- $v = c_0 + c_1 x_i + c_2 x_i^2 + \cdots + c_{p^i d-1} x_i^{p^i d-1}$ with $c_i \in \mathbb{F}_p$.

How much does it cost to...

- Multiply?
- Express the embedding $\mathbb{U}_{i-1} \subset \mathbb{U}_i$?
- Express the vector space isomorphism $\mathbb{U}_i = \mathbb{U}_{i-1}^p$?
- Switch between the representations?

A primitive tower

$$\begin{array}{c} \mathbb{U}_k \\ | \\ \mathbb{U}_{k-1} \\ \vdots \\ \mathbb{U}_1 \\ | \\ \mathbb{U}_0 \end{array}$$

Definition (Primitive tower)

A tower is primitive if $\mathbb{U}_i = \mathbb{F}_p[X_i]$.

In general this is not the case. Think of $P_0 = X^p - X - 1$.

Theorem (extends a result in [Cantor '89])

Let $x_0 = X_0$ *such that* $\mathrm{Tr}_{\mathbb{U}_0/\mathbb{F}_p}(x_0) \neq 0$ *, let*

$$\begin{aligned} P_0 &= X^p - X - x_0 \\ P_i &= X^p - X - x_i^{2p-1} \end{aligned}$$

with x_{i+1} *a root of* P_i *in* $\mathbb{U}_{i+1}$.
Then, the tower defined by $(P_0, \ldots, P_{k-1})$ *is primitive.*

Some tricks to play when $p = 2$.

We look for Q_i, the minimal polynomial of x_i over $\mathbb{F}_p$

$\mathbb{U}_k$

$\mathbb{U}_{k-1}$

$\mathbb{U}_1$

$\mathbb{U}_0$

Algorithm [Cantor '89]

- $Q_0 = Q$ easy,
- $Q_1 = Q_0(X^p - X)$ easy,

Let ω be a $2p-1$-th root of unity,

- $q_{i+1}(X^{2p-1}) = \prod_{j=0}^{2p-2} Q_i(\omega^j X)$ not too hard[a],
- $Q_{i+1} = q_{i+1}(X^p - X)$ easy.

[a] No need to factor Φ_{2p-1}, one can simply work modulo it. (Proof by Chinese remindering)

Complexity

$$O\left(\mathsf{M}(p^{i+2}d)\log p\right)$$

Level embedding

$\mathbb{U}_k$

$\mathbb{U}_{k-1}$

$\mathbb{U}_1$

$\mathbb{U}_0$

Push-down

Input $v \dashv \mathbb{U}_i$,
Output $v_0, \ldots, v_{p-1} \dashv \mathbb{U}_{i-1}$ such that $v = v_0 + \cdots + v_{p-1} x_i^{p-1}$.

Lift-up

Input $v_0, \ldots, v_{p-1} \dashv \mathbb{U}_{i-1}$,
Output $v \dashv \mathbb{U}_i$ such that $v = v_0 + \cdots + v_{p-1} x_i^{p-1}$.

Complexity function $\mathsf{L}(i)$

It turns out that the two operations lie in the same complexity class, we note $\mathsf{L}(i)$ for it:

$$\mathsf{L}(i) \ = \ O\left(p\mathsf{M}(p^i d) + p^{i+1} d \log_p (p^i d)^2\right)$$

Level embedding

Change of order

$$\begin{cases} X_i^p - X_i - X_{i-1}^{2p-1} = 0 \\ Q_{i-1}(X_{i-1}) = 0 \end{cases} \qquad \leftrightarrow \qquad \begin{cases} Q_i(X_i) = 0 \\ X_{i-1} = R(X_i)/S(X_i) \end{cases}$$

Rational Univariate Representation ([Rouillier '99])

- Push-down: left-to-right,
- Lift-up: right-to-left,
- going right-to-left $=$ looking for RUR,
- equivalently, changing from *lex* to *revlex* order.
- Many optimisations for finite fields case.

Push-down

Input $v \dashv \mathbb{U}_i$,
Output $v_0, \ldots, v_{p-1} \dashv \mathbb{U}_{i-1}$ s.t. $v = v_0 + \cdots + v_{p-1} x_i^{p-1}$.

1. Reduce v modulo $x_i^p - x_i - T^{2p-1}$ by a divide-and-conquer approach,
2. each of the coefficients of x_i has degree in x_{i-1} less than $2\deg(v)$,
3. reduce each of the coefficients.

Duality I

Dual vector space

$\mathbb{U}_i^*$ the space of $\mathbb{F}_p$-linear forms over $\mathbb{U}_i$

$$
\begin{aligned}
B \text{ base of } \mathbb{U}_i \quad &\rightarrow \quad B^* \text{ base of } \mathbb{U}_i^* \\
\ell \in \mathbb{U}_i^* \quad &\rightarrow \quad (\ell(B_0), \dots, \ell(B_n))
\end{aligned}
$$

Multiplication

Let $v \in \mathbb{U}_i$, multiplication by v is a linear application $\mathbb{U}_i \rightarrow \mathbb{U}_i$ with matrix M_v:

$$\begin{pmatrix} & & \\ & M_v & \\ & & \end{pmatrix} \begin{pmatrix} \\ x \\ \\ \end{pmatrix} \mapsto \begin{pmatrix} \\ vx \\ \\ \end{pmatrix}$$

Transposed multiplication

Let $v \in \mathbb{U}_i$, $\ell \in \mathbb{U}_i^*$, transposed multiplication $v \cdot \ell$ is the linear form

$$\begin{pmatrix} & v \cdot \ell & \end{pmatrix} \begin{pmatrix} \\ x \\ \\ \end{pmatrix} = \begin{pmatrix} & \ell & \end{pmatrix} \begin{pmatrix} & & \\ & M_v & \\ & & \end{pmatrix} \begin{pmatrix} \\ x \\ \\ \end{pmatrix} \mapsto \begin{pmatrix} & \ell & \end{pmatrix} \begin{pmatrix} \\ vx \\ \\ \end{pmatrix} = \ell(vx)$$

hence M_v^T is the linear application computing $v \cdot \ell$ from ℓ.

Duality II

Change of basis

Vector spaces $V^B = V^D$ with bases B and D.

$$M : V^B \to V^D$$
$$M^T : V^{D^*} \to V^{B^*}$$

M^T is the dual change of basis.

Push-down

Push-down is a change of basis
$P : \mathbb{U}_i^U \to \mathbb{U}_i^D$

$$U = \text{ polynomial basis in } x_i$$
$$D = \text{ bivariate basis in } x_i, x_{i-1}$$

hence $P^T : \mathbb{U}_i^{D^*} \to \mathbb{U}_i^{U^*}$.

Truncated power series

P^T sends linear forms $\ell \in \mathbb{U}_i^{D^*}$ onto the basis U^*:

$$\ell(1), \quad \ell(x_i), \quad \ell(x_i^2), \quad \ldots, \quad \ell(x_i^{p^i d-1})$$

These can be seen as the first coefficients of a formal power series ([Shoup '99]):

$$\sum_{j>0} \ell(x_i^j) Z^j$$

Dualities and transposition principle

"From every *linear algorithm* computing a linear application we can deduce another *linear algorithm* computing the transpose application using *about* the same space and time resources."

Category theory justification

$$
\begin{tikzcd}
 & {} \arrow[r] \arrow[dr, phantom, "C_2"] & {} \arrow[dr] & & {} \arrow[r] \arrow[dr, phantom, "C_1"] & {} \arrow[dr] & \\
a \arrow[ur] \arrow[rrr, dashed, "f_2"'] & & & b \arrow[ur] \arrow[rrr, dashed, "f_1"'] & & & c
\end{tikzcd}
$$

Lift-up

Trace formulae [Pascal, Schost '06, Rouillier '99]

Let $\mathrm{Tr} \in \mathbb{U}_i^{D^*}$ be the trace form, let $v_D \in \mathbb{U}_i^D$, then

$$\sum_{j>0} v_D \cdot \mathrm{Tr}(x_i^j) Z^j = \frac{N_v(Z)}{\operatorname{rev} Q_i(Z)}$$

is in $\mathbb{F}_p(Z)$. Then the image of v_D in $\mathbb{U}_i^U$ is

$$v_U = \frac{\operatorname{rev} N_v(x_i)}{Q_i'(Z)} \bmod Q_i(Z).$$

Transposition principle (see [Bürgisser, Clausen, Shokrollahi])

- We don't bother computing the matrices M_v and P,
- we use transposition principle instead.
- computing $v_D \cdot \mathrm{Tr}$ is transposed multiplication in $\mathbb{U}_i^D$,
- computing the power series is transposed Push-down.

Lift-up

Input $v_0, \ldots, v_{p-1} \dashv \mathbb{U}_{i-1}$
Output $v \dashv \mathbb{U}_i$ s.t. $v = v_0 + \cdots + v_{p-1} x_i^{p-1}$

1. Compute the linear form $\mathrm{Tr} \in \mathbb{U}_i^{D^*}$,
2. compute $\ell = (v_0 + \cdots + v_{p-1} x_i^{p-1}) \cdot \mathrm{Tr}$,
3. compute $P_v = \text{Push-down}^T(\ell)$,
4. compute $N_v(Z) = P_v(Z) \cdot \mathrm{rev}(Q_i)(Z) \mod Z^{p^i d - 1}$,
5. return $\mathrm{rev}(N_v)/Q_i' \mod Q_i$.

Speeding up some arithmetics

$\mathbb{U}_k$

$\mathbb{U}_{k-1}$

$\mathbb{U}_1$

$\mathbb{U}_0$

Divide and conquer

We improve some operations in $\mathbb{U}_i$ $\quad\quad \mathrm{op}(v)$

Where it works

- traces,
- p-th roots,
- pseudotraces,
- inversion,
- iterated frobenius,
- ...

Speeding up some arithmetics

$$\begin{array}{c} \mathbb{U}_k \\ | \\ \mathbb{U}_{k-1} \\ \vdots \\ \mathbb{U}_1 \\ | \\ \mathbb{U}_0 \end{array}$$

Divide and conquer

We improve some operations in $\mathbb{U}_i$

- push-down the operands;

$$\begin{array}{c} \mathrm{op}(v) \\ \downarrow \\ v_0, \quad \ldots, \quad v_{p-1} \end{array}$$

Where it works

- traces,
- p-th roots,
- pseudotraces,
- inversion,
- iterated frobenius,
- ...

Speeding up some arithmetics

$$\mathbb{U}_k \;—\; \mathbb{U}_{k-1} \;-\,-\,-\; \mathbb{U}_1 \;—\; \mathbb{U}_0$$

Divide and conquer

We improve some operations in $\mathbb{U}_i$

- push-down the operands;
- recursively solve p instances in $\mathbb{U}_{i-1}$;

$$\begin{array}{c} \mathrm{op}(v) \\ \downarrow \\ \mathrm{op}(v_0), \quad \dots, \quad \mathrm{op}(v_{p-1}) \end{array}$$

Where it works

- traces,
- p-th roots,
- pseudotraces,
- inversion,
- iterated frobenius,
- ...

Speeding up some arithmetics

$$\begin{tikzcd}
\mathbb{U}_k \arrow[d, dash] \\
\mathbb{U}_{k-1} \arrow[d, dash, dashed] \\
\mathbb{U}_1 \arrow[d, dash] \\
\mathbb{U}_0
\end{tikzcd}$$

Divide and conquer

We improve some operations in $\mathbb{U}_i$

- push-down the operands;
- recursively solve p instances in $\mathbb{U}_{i-1}$;
- combine the results;

$$\begin{tikzcd}
 & \mathrm{op}(v) \arrow[d] & \\
\mathrm{op}(v_0), \arrow[drr] & \dots, \arrow[d] & \mathrm{op}(v_{p-1}) \arrow[dll] \\
w_0, & \dots, & w_{p-1}
\end{tikzcd}$$

Where it works

- traces,
- p-th roots,
- pseudotraces,
- inversion,
- iterated frobenius,
- ...

Speeding up some arithmetics

$\mathbb{U}_k$

$\mathbb{U}_{k-1}$

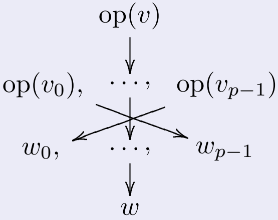
$\mathbb{U}_1$

$\mathbb{U}_0$

Divide and conquer

We improve some operations in $\mathbb{U}_i$

- push-down the operands;
- recursively solve p instances in $\mathbb{U}_{i-1}$;
- combine the results;
- lift-up.



Where it works

- traces,
- p-th roots,
- pseudotraces,
- inversion,
- iterated frobenius,
- ...

Example: Iterated frobenius

Truisms

- $x_i^{p^{p^j d}} = x_i + \beta_{i-1,j}$ where $\beta_{i-1,j} = \sum_{h=0}^{p^j d-1} (x_{i-1}^{2p-1})^{p^h}$,
- $v \in \mathbb{U}_i \;\Rightarrow\; v^{p^{p^i d}} = v$,
- $v^{p^{p^j d}} = \sum_{h=0}^{p-1} v_h^{p^{p^j d}} (x_i + \beta_{i-1,j})^h$

IterFrobenius

Input v, i, j with $v \dashv \mathbb{U}_i$ and $j \geqslant 0$.
Output $v^{p^{p^j d}} \dashv \mathbb{U}_i$.

1. If $i \leqslant j$, return v.
2. Let $v_0 + v_1 x_i + \cdots + v_{p-1} x_i^{p-1} = \text{Push-down}(v)$,
3. for $h \in [0, \ldots, p-1]$, let $t_h = \text{IterFrobenius}(v_h, i-1, j)$,
4. let $w = \sum_{h=0}^{p-1} t_h (x_i + \beta_{i-1,j})^h$,
5. return Lift-up(w).

Example: Iterated frobenius $O\left((i-j)\mathsf{L}(i)\right)$

Truisms

- $x_i^{p^{p^j d}} = x_i + \beta_{i-1,j}$ where $\beta_{i-1,j} = \sum_{h=0}^{p^j d-1} (x_{i-1}^{2p-1})^{p^h}$,
- $v \in \mathbb{U}_i \;\Rightarrow\; v^{p^{p^i d}} = v$,
- $v^{p^{p^j d}} = \sum_{h=0}^{p-1} v_h^{p^{p^j d}} (x_i + \beta_{i-1,j})^h$

IterFrobenius

Input v, i, j with $v \dashv \mathbb{U}_i$ and $j \geqslant 0$.
Output $v^{p^{p^j d}} \dashv \mathbb{U}_i$.

1. If $i \leqslant j$, return v.
2. Let $v_0 + v_1 x_i + \cdots + v_{p-1} x_i^{p-1} = \text{Push-down}(v)$,
3. for $h \in [0, \ldots, p-1]$, let $t_h = \text{IterFrobenius}(v_h, i-1, j)$,
4. let $w = \sum_{h=0}^{p-1} t_h (x_i + \beta_{i-1,j})^h$,
5. return $\text{Lift-up}(w)$.

Important example : Generic towers

$\mathbb{U}_k$

$\mathbb{U}_{k-1}$

$\mathbb{U}_1$

$\mathbb{U}_0$

Generic towers

- Let $(\alpha_0, \ldots, \alpha_{k-1})$ define a generic tower over $\mathbb{U}_0$,
- if we find an isomorphism we can bring fast arithmetics to it.

Computing the isomorphism [Couveignes '00]

Goal: factor $X^p - X - \alpha_i$ in U_{i+1}.

- Change of variables $X' = X - \mu$ s.t.
- $X'^p - X' - \alpha_i$ has a root in $\mathbb{U}_i$,
- Push-down, solve recursively, result is Δ,
- Lift-up Δ,
- return $\Delta + \mu$.

$\mathbb{U}'_k$

$\mathbb{U}'_{k-1}$

$\mathbb{U}'_1$

$\mathbb{U}_0$

Implementation

Implementation in NTL

Three types

- GF2: $p = 2$, no FFT, bit optimisation,
- zz_p: $p < 2^{|\texttt{long}|}$, FFT, no bit-tricks,
- ZZ_p: generic p, like zz_p but slower.

Comparison to Magma

Three ways of handling field extensions

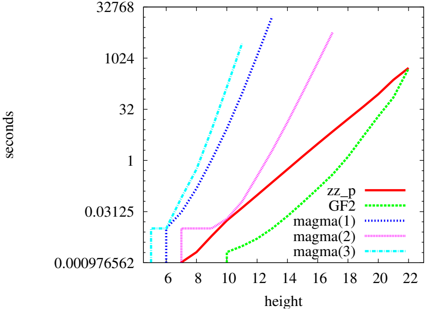
1. quo<U|P>: quotient of multivariate polynomial ring + Gröbner bases
2. ext<k|P>: field extension by $X^p - X - \alpha$, precomputed bases + multivariate
3. ext<k|p>: field extension of degree p, precomputed bases + multivariate

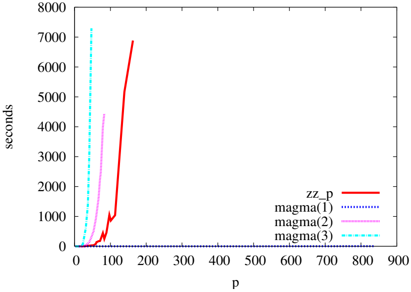
Benchmarks (on 14 AMD Opteron 2500)

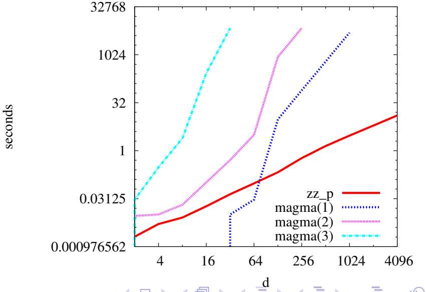
Three modes

- $p = 2$, $d = 1$, height varying,
- p varying, $d = 1$, height $= 2$,
- $p = 5$, d varying, height $= 2$.

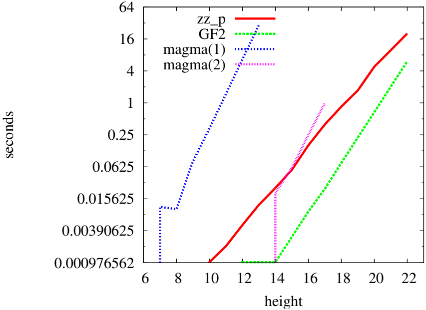
Construction of the tower + precomputations

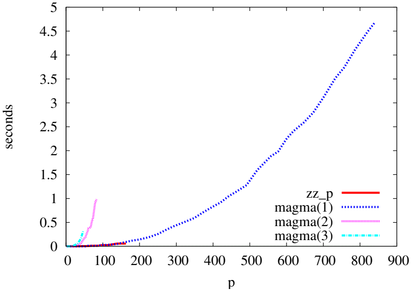


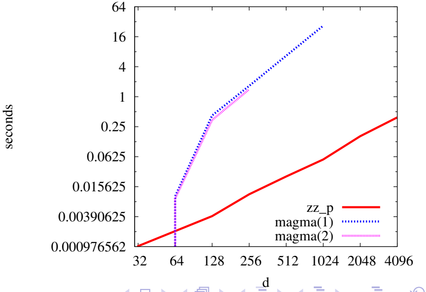




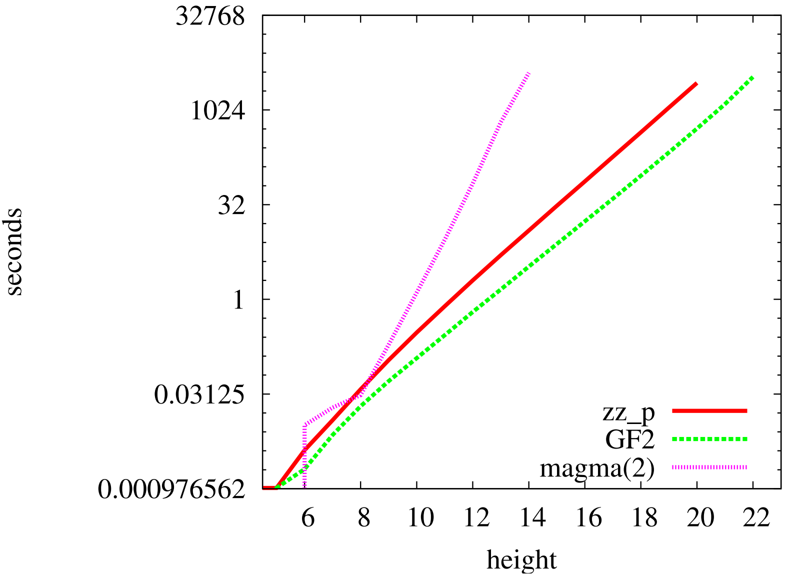
Multiplication





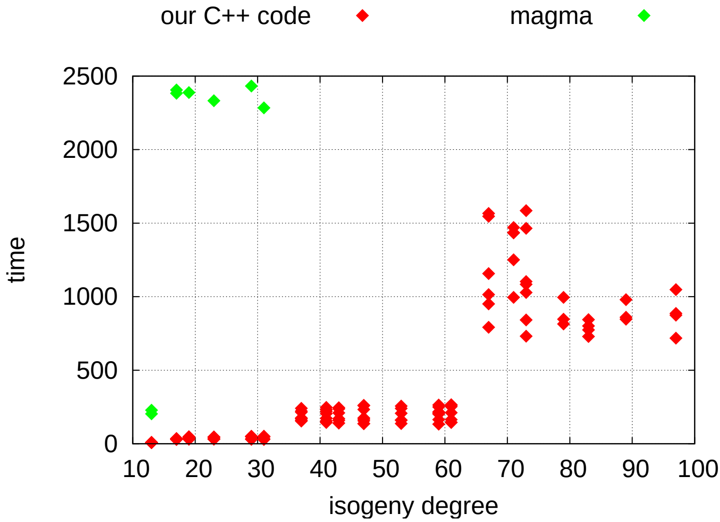


Isomorphism ([Couveignes '00] vs Magma)



Benchmarks on isogenies ([Couveignes '96])

Over $\mathbb{F}_{2^{101}}$, on an AMD Athlon 64 X2 Dual Core Processor 4000+, 5GB ram



Bibliography

P. Bürgisser, M. Clausen, and A. Shokrollahi.
Algebraic complexity theory, volume 315 of *Grundlehren Math. Wiss.*
Springer–Verlag, 1997.

D. G. Cantor.
On arithmetical algorithms over finite fields.
Journal of Combinatorial Theory, Series A 50, 285-300, 1989.

J.-M. Couveignes.
Computing ℓ-isogenies with the p-torsion.
Lecture Notes in Computer Science vol. 1122, pages 59–65, Springer-Verlag, 1996.

J.-M. Couveignes.
Isomorphisms between Artin-Schreier tower.
Math. Comp. 69(232): 1625–1631, 2000.

L. De Feo.
Calcul d'isogénies.
Master thesis. http://www.lix.polytechnique.fr/∼defeo

Bibliography

C. Pascal and É. Schost.
Change of order for bivariate triangular sets.
In *ISSAC'06*, pages 277–284. ACM, 2006.

F. Rouillier.
Solving zero-dimensional systems through the Rational Univariate Representation.
Appl. Alg. in Eng. Comm. Comput., 9(5):433–461, 1999.

V. Shoup.
Efficient computation of minimal polynomials in algebraic extensions of finite fields.
In *ISSAC'99*, ACM Press, 1999.

J.F. Voloch.
Explicit p-descent for Elliptic Curves in Characteristic p.
Compositio Mathematica 74, pages 247–58, 1990.