Fast arithmetics for Artin-Schreier extensions

L. De Feo
joint work with Éric Schost

École Polytechnique, Paris, France

December 7, 2008
CMS Winter Meeting, Ottawa

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

$$
\begin{tikzcd}
\mathbb{U}_k = \dfrac{\mathbb{U}_{k-1}[X_k]}{P_{k-1}(X_k)} \arrow[d, dash, "p"] \\
\mathbb{U}_{k-1} \arrow[d, dash, dashed] \\
\mathbb{U}_1 = \dfrac{\mathbb{U}_0[X_1]}{P_0(X_1)} \arrow[d, dash, "p"] \\
\mathbb{U}_0 = \mathbb{F}_{p^d} = \dfrac{\mathbb{F}_p[X_0]}{Q(X_0)}
\end{tikzcd}
$$

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].

Plan

Representation matters!

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

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.*

Proof (...kind of)

Lemma

Let x be the generator of an Artin-Schreier extension $\mathbb{L}/\mathbb{K}$, then for $0 < j < 2p - 1$

$$\operatorname{Tr}_{\mathbb{L}/\mathbb{K}}(x^j) = \begin{cases} -1 & \textit{if } j = p-1 \textit{ or } j = 2p-2. \\ 0 & \textit{elsewhere.} \end{cases}$$

Irreducibility

- $x_i^{2p-1} = x_i^p x_i^{p-1} = (x_i + x_{i-1}^{2p-1})x_i^{p-1} = x_i + x_{i-1}^{2p-1} + x_i^{p-1}x_{i-1}^{2p-1}$,
- $\operatorname{Tr}_{\mathbb{U}_i/\mathbb{U}_{i-1}}(x_i^{2p-1}) \; = \; -x_{i-1}^{2p-1}$,
- conclude by composition of traces.

Primitivity

Same idea but use a linear application extending the trace beyond $\mathbb{U}_i$.

Some tricks to play when $p = 2$.

Computing the minimal polynomials

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

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,

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

[1] No need to factor Φ_{2p-1}, one can simply work modulo it.

Complexity

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

Plan

Level embedding

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:

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

Push-down

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.

Lift-up

Power projection

Let x be fixed. An algorithm that takes a linear form ℓ as input and outputs

$$\ell(1)\ ,\ \ell(x)\ ,\ \dots\ ,\ \ell(x^n)$$

is said to solve *power projection* problem ([Shoup '99]).

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

- Given $v_0, \dots, v_{p-1} \dashv \mathbb{U}_{i-1}$,
- $v = v_0 + \cdots + v_{p-1}x_i^{p-1}$ can be recovered using suitable trace formulas.
- Solving them is the power projection problem on inputs Tr and $v \cdot \mathrm{Tr}$.

Transposed algorithms (see [Bürgisser, Clausen, Shokrollahi])

- *Linear algorithms* can be *transposed* much like linear applications;
- Computing $v \cdot \mathrm{Tr}$ is *transposed multiplication*.
- Computing the power projection for x_i is *transposed push-down*.

Other operations, Isomorphism

Other operations

Using divide and conquer, we can give efficient routines for most operations in $\mathbb{U}_i$:

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

It works fairly well for

- inversion,
- traces,
- iterated frobenius,
- square roots? (work in progess)
- ...

Isomorphism [Couveignes '00]

- Let $(\alpha_0, \ldots, \alpha_{k-1})$ define another tower over $\mathbb{U}_0$,
- factoring $X^p - X - \alpha_i$ in $\mathbb{U}_{i+1}$ gives an isomorphism.
- Couveignes gives a fast factoring algorithm for this case,
- this way fast arithmetics can be brought to this new tower.

Plan

1. Representation
2. Arithmetics
3. Applications and implementation

p^k-torsion

p-division

- In ordinary elliptic curves $E[p^k] \simeq \mathbb{Z}/p^k\mathbb{Z}$.
- Knowing a p^i-torsion point,
- factorise the p-division polynomial to find a p^{i+1}-torsion point.

Make it Artin-Schreier [Voloch '90]

- By a change of variables we can factor an Artin-Schreier polynomial instead,
- using Couveignes' algorithm for the isomorphism, we can do it efficiently.

Isogeny interpolation

Computing an isogeny of degree ℓ between two curves E and F

The idea [Couveignes '96, '00]

- Compute enough ($p^k \sim \ell$) torsion points in E and F,
- since the curves are isogenous, the towers are isomorphic,
- use the isomorphism algorithm to bring them to the same primitive tower,
- interpolate the isogeny over the points.

Fast interpolation [D.F. '07]

- Use the same divide-and-conquer approach as for the arithmetics in $\mathbb{U}_k$,
- throw some Galois-theory in,
- the interpolation step can be done in $\tilde{O}(\ell^2)$.

Implementation

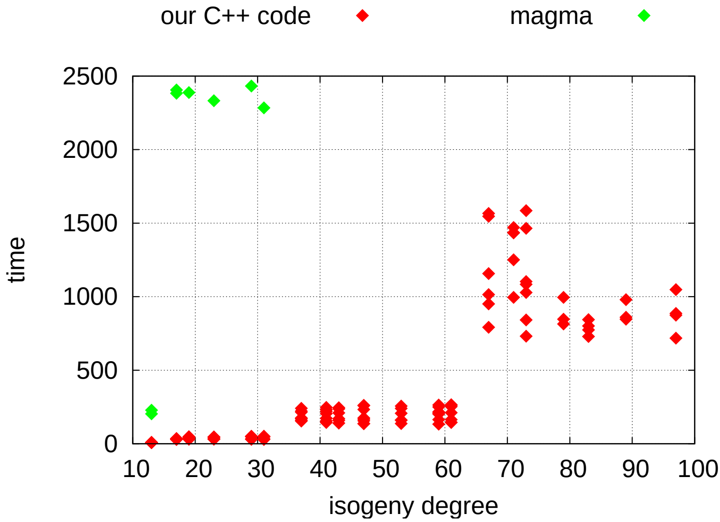
- Implementation in NTL for $p = 2$ (no FFT).
- Benchmarks on two fields: $\mathbb{F}_{2^{101}}$ and $\mathbb{F}_{2^{1999}}$.
- Up to 15 levels on a Intel Core 2 @2GHz, 4GB ram.

	$\mathbb{F}_{2^{101}}$	$\mathbb{F}_{2^{1999}}$	levels
Construction of Q_i	$0:42$	$42:00$	15
Push-down, lift-up	$0:30$	$20:00$	15
Couveignes '00	$3:40:00$		15
Couveignes '00	$1:30:00$	$76:40:00$	13

- We are working on a new, faster, NTL implementation for any p;
- porting to a computer algebra platform is in study.

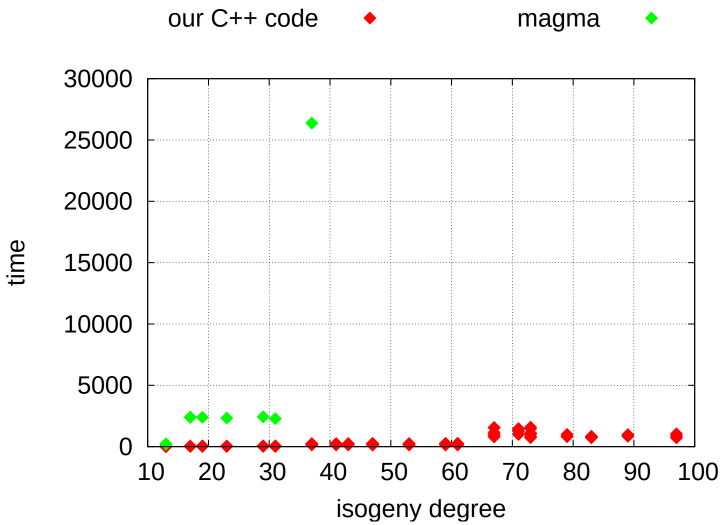
Benchmarks on isogenies

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



Benchmarks on isogenies

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.