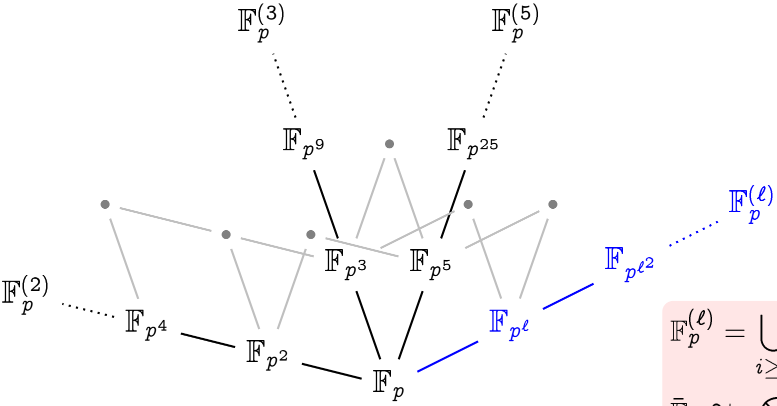
UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

ALGORITHMS FOR $\bar{\mathbb{F}}_p$

Luca De Feo[1]
joint work with Javad Doliskani[2] and Éric Schost[2]
[1]Université de Versailles – Saint-Quentin-en-Yvelines
[2]University of Western Ontario

Séminaire BAC, September 20, 2013

What does $\bar{\mathbb{F}}_p$ look like?



$$\mathbb{F}_p^{(\ell)} = \bigcup_{i\geq 0} \mathbb{F}_{p^{\ell^i}},$$

$$\bar{\mathbb{F}}_p \cong \bigotimes_{\ell \text{ prime}} \mathbb{F}_p^{(\ell)}$$

In software

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

Definition (Compatible lattice)

- A collection of finite fields $\mathbb{F}_{p^n}$ for any $n \geq 1$;
- A collection of morphisms $\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$ whenever $m|n$.

Fact

Given a lattice, any element of $\bar{\mathbb{F}}_p$ can be represented as an element of a finite field in the lattice.

(Lenstra, De Smit & Lenstra) $\Omega(n^3)$

There exist a determinisitic algorithm that constructs a compatible lattice in time polynomial in $\log p$ and n, where n is the degree of the largest computed extension of $\mathbb{F}_p$.

Our interest

- Efficient construction of lattices,
- Efficient field operations.

Goals:

- Constructing fields:
  - Build irreducible polynomials in quasi-linear time.
- Describing embeddings:
  - Quasi-linear time and memory in the degree of the extension.
- Evaluating embeddings:
  - Replace linear algebra by polynomial arithmetic.

Application examples:

- General: finite field arithmetic, unramified extensions of $\mathbb{Q}_p$.
- Computing isogenies between elliptic curves, DF, 2011.
- Point-counting in genus 2, Gaudry and Schost, 2012.

Known constructions

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

Construct fields arbitrarily + compute embeddings

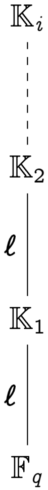
- Describe the embeddings
  - Factor minimal polynomials,
  - Allombert's isomorphism algorithm (in Pari?).
  - Rains' isomorphism algorithm (unpublished, in Magma),
- Evaluate the embeddings
  - Linear algebra,
  - Map generators (polynomial arithmetic).

Construct fields defined by special polynomials

- (pseudo)-Conway polynomials,
- Cyclotomy theory (De Smit & Lenstra and generalizations),
- Fancy (and still limited) constructions (this talk).

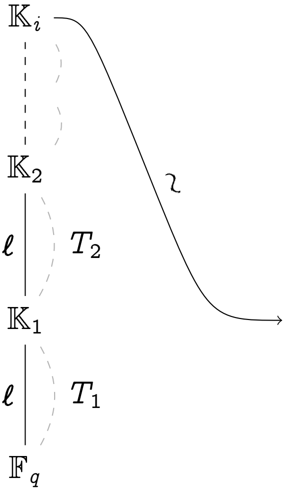
Towers

Univariate vs. Multivariate



$$\mathbb{F}_q[X_i]/Q_i(X_i)$$

$$\mathbb{F}_q[X_1, X_2, \ldots, X_i]/\left|\begin{array}{r} T_i(X_i, \ldots, X_2, X_1) \\ \vdots \\ T_2(X_2, X_1) \\ T_1(X_1) \end{array}\right.$$

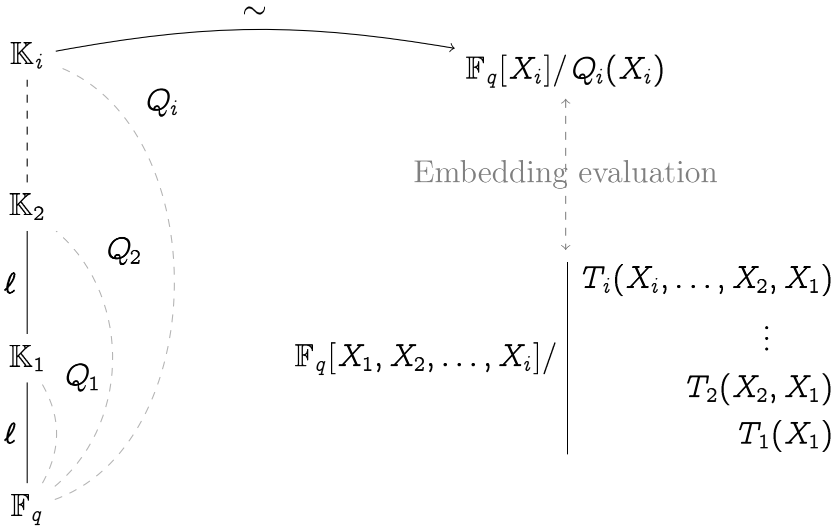


$$\mathbb{F}_q[X_i]/Q_i(X_i)$$

$$\mathbb{F}_q[X_1, X_2, \dots, X_i] \Big/ \left| \begin{array}{r} T_i(X_i, \dots, X_2, X_1) \\ \vdots \\ T_2(X_2, X_1) \\ T_1(X_1) \end{array} \right.$$

Univariate vs. Multivariate

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES



Summary of Main Results

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

Previous work

- Artin-Schreier (Cantor, Couveignes, DF & Schost): q fixed, $\ell = p$ small;
- Dyadic towers (Doliskani & Schost): q fixed, $\ell = 2$;
- $\tilde{O}(\ell^{i+c})$ operations in $\mathbb{F}_q$, $c \in \{1,2\}$.

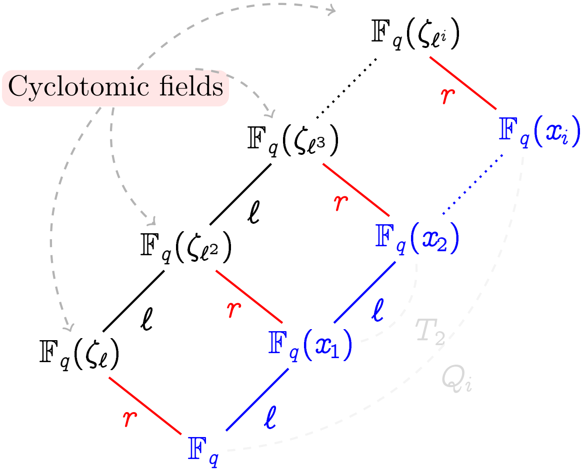
This work: objective

- q fixed, ℓ small: $\tilde{O}(\ell^i)$ operations in $\mathbb{F}_q$;
- Limit additional factors in ℓ and q as much as possible.

Condition	Initialization	$\mathbf{Q_i}, \mathbf{T_i}$	Embedding eval.
$q = 1 \bmod \ell$	$O(1)$	$O(\ell^i)$	$O(\ell^i)$
$q = -1 \bmod \ell$	$O(1)$	$O(\ell^i)$	$O(\mathrm{M}(\ell^i)\log(\ell^i))$
–	$O(\ell^2)$	$O(\mathrm{M}(\ell^{i+1})\mathrm{M}(\ell)\log(\ell^i)^2)$	$O(\mathrm{M}(\ell^{i+1})\mathrm{M}(\ell)\log(\ell^i))$
$4\ell \leq q^{1/4}$	$\tilde{O}(\ell^3)$ (bit)	$O(\mathrm{M}(\ell^i)\log(\ell^i))$	$O(\mathrm{M}(\ell^i)\log(\ell^i))$
$4\ell \leq q^{1/4}$	$\tilde{O}(\mathrm{M}(\ell))$	$O(\mathrm{M}(\ell^i)\log(\ell^i))$	$O(\mathrm{M}(\ell^i)\log(\ell^i))$

Quasi-cyclotomic towers

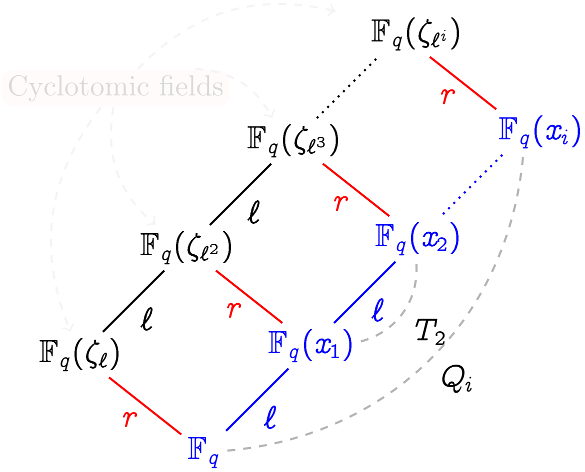
(inspired by Shoup, Allombert, De Smit and Lenstra)



- $r \mid (\ell - 1)$;
- $x_i = \mathrm{Tr}_{\mathbb{K}_i/\mathbb{F}_{q^{\ell^i}}}(\zeta_{\ell^i})$;
- Both T_i and Q_i can be computed by resultants.

Quasi-cyclotomic towers

(inspired by Shoup, Allombert, De Smit and Lenstra)



- $r \mid (\ell - 1)$;
- $x_i = \mathrm{Tr}_{\mathbb{K}_i/\mathbb{F}_{q^{\ell^i}}}(\zeta_{\ell^i})$;
- Both T_i and Q_i can be computed by resultants.

Quasi-cyclotomic towers

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

Generic algorithm

- Perform all computations in the cyclotomic tower;
- Construction and embedding evaluation: penalty only $\tilde{O}(\ell^2)$.

Trivial case: $\ell \mid (q-1) \Leftrightarrow r = 1$

Kummer extensions

$$Q_i = X_i^{\ell^i} - y_0 \qquad \text{and} \qquad T_i = X_i^{\ell} - X_{i-1}$$

Embeddings are trivial.

Quasi-cyclotomic towers

Generic algorithm

- Perform all computations in the cyclotomic tower;
- Construction and embedding evaluation: penalty only $\tilde{O}(\ell^2)$.

Special case: $\ell \mid (q+1) \Leftrightarrow r = 2$

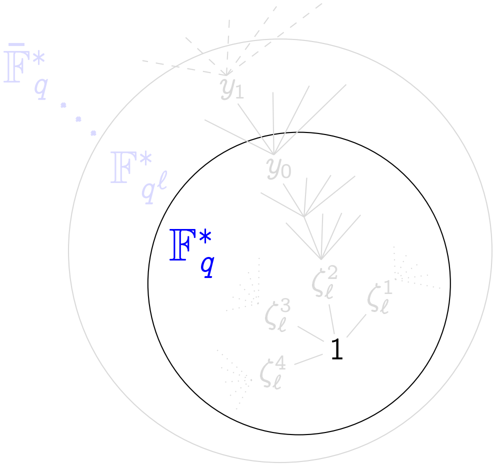
By direct resultant computation

$$Q_i(X_i) = Y^{\ell^i} + Y^{-\ell^i} - x_0 \mod Y^2 - X_i Y + 1$$

- Similar form for T_i.
- Q_i can be computed in $O(\mathrm{M}(\ell^i))$; a better algorithm later.
- Embeddings: later.

Towers from irreducible fibers (Couveignes and Lercier, 2011)

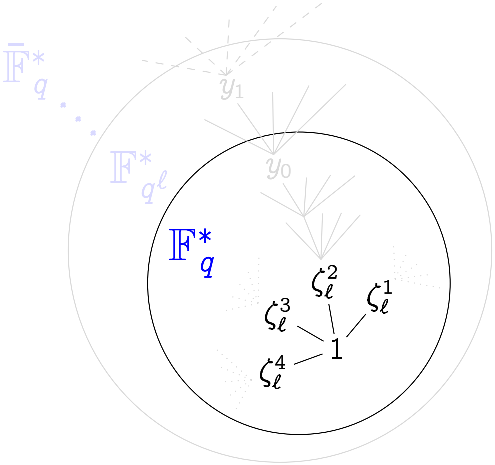
$\ell \mid (q-1)$, consider the map $\phi : x \mapsto x^\ell$



- $\phi|_{\mathbb{F}_q^*}$ not surjective;
- $\phi : \mathbb{G}_m \to \mathbb{G}_m$ surjective;
- Starting from y_0, every $\phi^{-1} y_i$ is an irreducible set of cardinality ℓ.

Towers from irreducible fibers (Couveignes and Lercier, 2011)

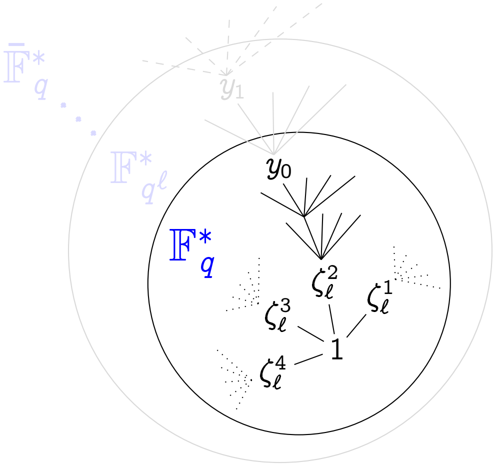
$\ell \mid (q-1)$, consider the map $\phi : x \mapsto x^\ell$



- $\phi|_{\mathbb{F}_q^*}$ not surjective;
- $\phi : \mathbb{G}_m \to \mathbb{G}_m$ surjective;
- Starting from y_0, every $\phi^{-1} y_i$ is an irreducible set of cardinality ℓ.

Towers from irreducible fibers (Couveignes and Lercier, 2011)

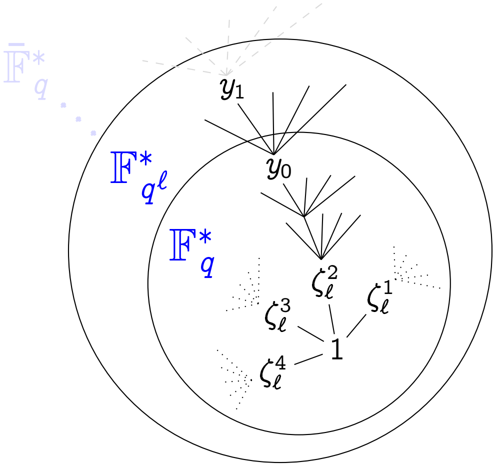
$\ell \mid (q-1)$, consider the map $\phi : x \mapsto x^\ell$



- $\phi|_{\mathbb{F}_q^*}$ not surjective;
- $\phi : \mathbb{G}_m \to \mathbb{G}_m$ surjective;
- Starting from y_0, every $\phi^{-1} y_i$ is an irreducible set of cardinality ℓ.

Towers from irreducible fibers (Couveignes and Lercier, 2011)

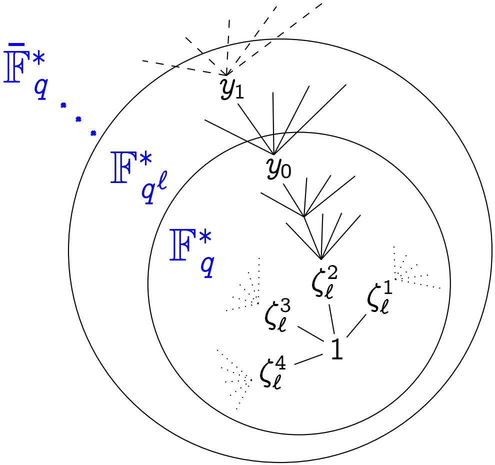
$\ell \mid (q-1)$, consider the map $\phi : x \mapsto x^\ell$



- $\phi|_{\mathbb{F}_q^*}$ not surjective;
- $\phi : \mathbb{G}_m \to \mathbb{G}_m$ surjective;
- Starting from y_0, every $\phi^{-1} y_i$ is an irreducible set of cardinality ℓ.

Towers from irreducible fibers (Couveignes and Lercier, 2011)

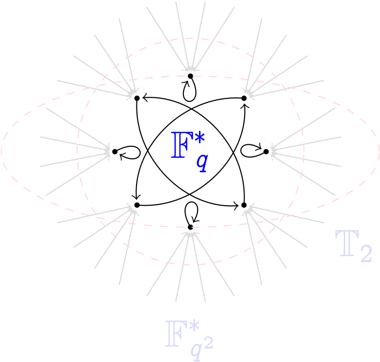
$\ell \mid (q-1)$, consider the map $\phi : x \mapsto x^\ell$



- $\phi|_{\mathbb{F}_q^*}$ not surjective;
- $\phi : \mathbb{G}_m \to \mathbb{G}_m$ surjective;
- Starting from y_0, every $\phi^{-1} y_i$ is an irreducible set of cardinality ℓ.

Chebyshev case: $\ell \mid (q+1)$

Consider the map $\phi : x \mapsto x^\ell$



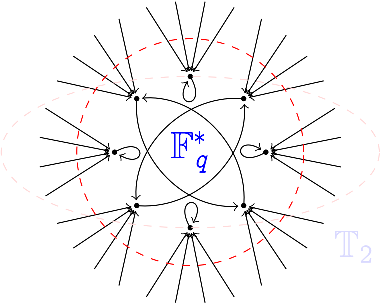
- $\phi|_{\mathbb{F}_q^*}$ bijective;
- $\phi|_{\mathbb{F}_{q^2}^*}$ non surjective;
- $\mathbb{T}_2 \subset \mathbb{F}_{q^2}^*$ algebraic torus of cardinality $q+1$.

$$\mathbb{T}_n(k) \cong \{\alpha \in L^* \mid \mathrm{N}_{L/F}(\alpha) = 1 \text{ for all } k \subset F \subsetneq L\}.$$

Chebyshev case: $\ell \mid (q+1)$

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

Consider the map $\phi : x \mapsto x^\ell$

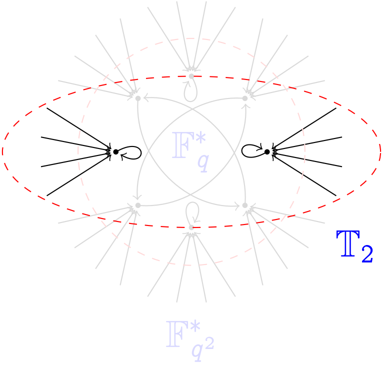


- $\phi|_{\mathbb{F}_q^*}$ bijective;
- $\phi|_{\mathbb{F}_{q^2}^*}$ non surjective;
- $\mathbb{T}_2 \subset \mathbb{F}_{q^2}^*$ algebraic torus of cardinality $q+1$.

$$\mathbb{T}_n(k) \cong \{\alpha \in L^* \mid \mathrm{N}_{L/F}(\alpha) = 1 \text{ for all } k \subset F \subsetneq L\}.$$

Chebyshev case: $\ell \mid (q+1)$

Consider the map $\phi : x \mapsto x^\ell$

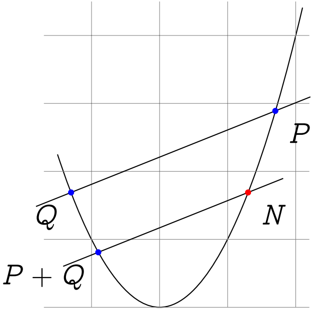


- $\phi|_{\mathbb{F}_q^*}$ bijective;
- $\phi|_{\mathbb{F}_{q^2}^*}$ non surjective;
- $\mathbb{T}_2 \subset \mathbb{F}_{q^2}^*$ algebraic torus of cardinality $q+1$.

$$\mathbb{T}_n(k) \cong \{\alpha \in L^* \mid \mathrm{N}_{L/F}(\alpha) = 1 \text{ for all } k \subset F \subsetneq L\}.$$

Towers from algebraic tori (Pell conics)

- By Weil descent, $\mathbb{T}_2$ is isomorphic to a Pell conic;
- Multiplication in $\bar{\mathbb{F}}_q$ induces a group law on the points.



Pell conic:

$$C \ : \ x^2 - \Delta y^2 = 4$$

Addition: For $P = (x_1, y_1)$ and $Q = (x_2, y_2)$,

$$P \oplus Q = \left(\frac{x_1 x_2 + \Delta y_1 y_2}{2}, \frac{x_1 y_2 + x_2 y_1}{2} \right)$$

Towers from algebraic tori

- $\mathbb{T}_2 \to$ Pell conic C,
- multiplication in $\mathbb{F}_{q^2} \to$ addition in C,
- ℓ-th power $\to$ scalar multiplication $[\ell]$.

Lemma

The abscissa of $[n]P$ is given by $C_n(x_1)$, where $C_n \in \mathbb{Z}[X]$ is the n-th Chebyshev polynomial.

Theorem

Let P be a point not in ℓC, then we can compute

$$Q_i(X_i) = C_{\ell^i}(X_i) - x_P \quad \text{and} \quad T_i(X_i) = C_\ell(X_i) - X_{i-1}$$

using $O(\ell^i)$ operations.

Towers from elliptic curves

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

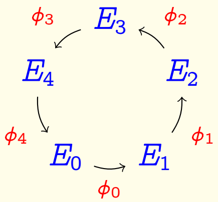
- Problem 1: there is essentially one conic; we would like to have more group choices, elliptic curves are an option.
- Problem 2: ℓ-multiplication on elliptic curves is a degree ℓ^2 map; we must consider separable isogenies instead.

$$E_0 \,:\, y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_q, \quad \ell \nmid (q-1), \quad \ell \mid \# E_0(\mathbb{F}_q)$$

Under these assumptions, isogenies form a cycle

$$\phi_i : E_i \to E_{i+1}.$$

Lemma $E_n \cong E_0$ for some $n \in O(\sqrt{q}\log(q))$.



Towers from elliptic curves

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

Lemma (Couveignes and Lercier, 2011)

Let $P \notin \ell E_i$, and $\psi = \phi_{i-1} \circ \phi_{i-2} \circ \cdots \circ \phi_j$,
then $\psi^{-1}(P)$ is irreducible of cardinality ℓ^{i-j}.

Vélu's formulas

$$\begin{array}{rccc} \phi_i : & E_i & \longrightarrow & E_{i+1}, \\ & (x, y) & \longmapsto & \left(\frac{f_i(x)}{g_i(x)}, y \left(\frac{f_i(x)}{g_i(x)} \right)' \right), \end{array}$$

The ℓ-adic tower

$$T_1 = f_{-1}(X_1) - \eta g_{-1}(X_1),$$
$$T_i = f_{-i}(X_i) - X_{i-1} g_{-i}(X_i).$$

Evaluating embeddings

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

Observation

In all previous cases, from the form of T_i we deduce

$$X_{i-1} = f(X_i)/g(X_i)$$

for some f and g. Going from multivariate to univariate is

$$\sum a_j X_{i-1}^{\alpha_j} X_i^{\beta_j} \mapsto \sum a_j \frac{f(X_i)^{\alpha_j}}{g(X_i)^{\alpha_j}} X_i^{\beta_j}$$

Definition

Let $P \in \mathbb{F}_q[X, Y]$ and $n \in \mathbb{N}$, with $\deg(P, X) < n$. Define

$$P[f, g, n] = g^{n-1} P\left(\frac{f}{g}, Y\right) \in \mathbb{F}_q[Y].$$

Lifting: Multivariate → Univariate

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

Algorithm 1 Compose

Require: $P \in \mathbb{F}_q[X, Y]$, $f, g \in \mathbb{F}_q[Y]$, $n \in \mathbb{N}$

```
if n = 1 then
    return P
else
    m ← ⌈n/2⌉
    Let P_0, P_1 be such that P = P_0 + X^m P_1
    Q_0 ← Compose(P_0, f, g, m)
    Q_1 ← Compose(P_1, f, g, n − m)
    Q ← Q_0 g^(n−m) + Q_1 f^m
    return Q
end if
```

Theorem

Algorithm 1 computes $Q = P[f, g, n]$ using $O(\mathrm{M}(\ell n)\log(n))$ operations in $\mathbb{F}_q$.

Pushing: Univariate → Multivariate

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

Algorithm 2 Decompose

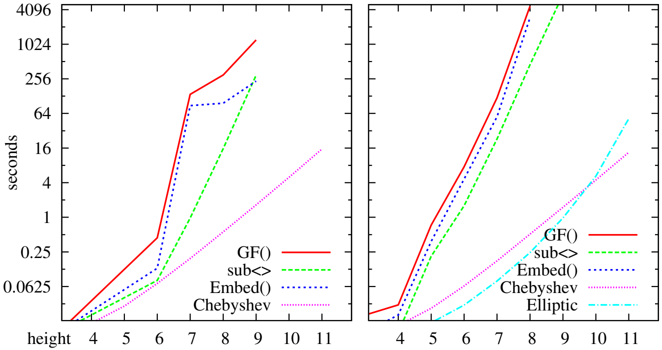
Require: $Q, f, g, h \in \mathbb{F}_q[Y]$, $n \in \mathbb{N}$

- **if** $n = 1$ **then**
  - **return** Q
- **else**
  - $m \leftarrow \lceil n/2 \rceil$
  - $u \leftarrow 1/g^{n-m} \bmod f^m$
  - $Q_0 \leftarrow Qu \bmod f^m$
  - $Q_1 \leftarrow (Q - Q_0 g^{n-m}) \operatorname{div} f^m$
  - $P_0 \leftarrow$ Decompose(Q_0, f, g, h, m)
  - $P_1 \leftarrow$ Decompose$(Q_1, f, g, h, n-m)$
  - **return** $P_0 + X^m P_1$
- **end if**

Theorem

Algorithm 2 computes a polynomial $P \in \mathbb{F}_q[X, Y]$ such that $Q = P[f, g, n]$ using $O(\mathsf{M}(\ell n)\log(n))$ operations in $\mathbb{F}_q$.

Implementation



Times for building 3-adic towers on top of $\mathbb{F}_2$ (left) and $\mathbb{F}_5$ (right), in Magma (first three lines) and using our code.

- Intel Xeon E5620 clocked at 2.4 GHz, using Sage 5.5 and Magma 2.18.12
- Source code at `https://github.com/defeo/towers`.

Lattices (work in progress)

Composita of fields

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

Input: $\mathbb{F}_{p^m} = \mathbb{F}_p[X]/P(X)$ and $\mathbb{F}_{p^m} = \mathbb{F}_p[Y]/P(Y)$, with $(m, n) = 1$.

Output: $\mathbb{F}_{p^{mn}} = \mathbb{F}_p[Z]/R(Z)$.

Theorem (Bostan & Schost)

Let x, y be roots of P, Q.

- Both xy and $x + y$ generate $\mathbb{F}_{p^{mn}}$;
- The minimal polynomial of xy or $x + y$ can be computed in $\tilde{O}(mn)$.

Towards quasi-optimal embeddings

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

Work in progress (with Doliskani and Schost)

- Evaluate the maps $\mathbb{F}_{p^n} \hookrightarrow \mathbb{F}_{p^{mn}}$; $\tilde{O}(mn)$
- Evaluate the sections; $\tilde{O}(mn)$
- Full pushing $\mathbb{F}_{p^{mn}} \to \mathbb{F}_{p^n}^m$. $\tilde{O}(mn\min(m,n))$

Techniques

- Bostan & Schost algorithm;
- Bivariate trace computations (following Rouiller);
- transposed algorithms (following Bostan, Salvy & Schost).

Summary

Results

- ℓ-adic towers very efficient for some ℓ;
- Asymptotically good for most small ℓ;
- Composita also asymptotically good;
- Full performances yet to test.

Open questions

- Large prime degree extensions;
- Quasi-optimal full push down in composita;
- Arbitrary finite field isomorphisms in proven/practical subquadratic time.