

# Fast algorithms for $\ell$ -adic towers over finite fields

Luca De Feo<sup>1</sup>, Javad Doliskani<sup>2</sup>, Éric Schost<sup>2</sup>

<sup>1</sup>Laboratoire PRiSM, Université de Versailles

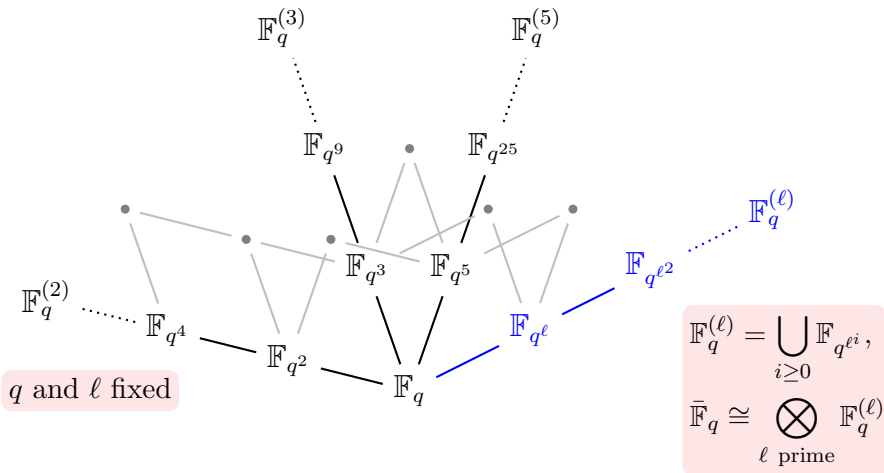
<sup>2</sup>Department of Computer Science, Western University

ISSAC, June 28, 2013



Find these slides, the paper and the source code on <http://defeo.lu/towers>

## Problem statement



## *Our interest*

- Efficient construction of towers
- Efficient computation of embeddings

## Goals:

- Describing embeddings:
  - ▶ Replace linear algebra by polynomial arithmetic.
- Computing embeddings:
  - ▶ Quasi-linear time and memory in the degree of the extension.

## Application examples:

- In general: finite field arithmetic.
- Computing isogenies between elliptic curves, L. De Feo, 2011.
- Point-counting in genus 2, Gaudry and Schost, 2012.

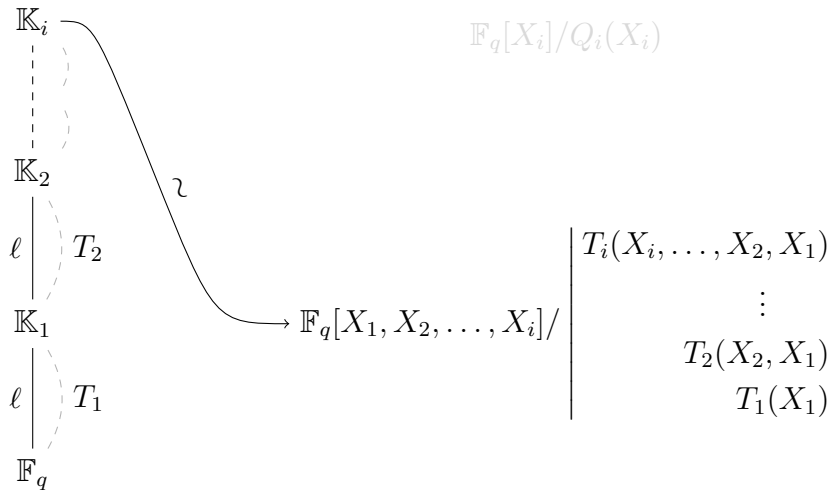
## Previous works

- Magma's implementation:
  - ▶ Bosma, Cannon, Steel, *Lattices of compatibly embedded finite fields*, 1997.
  - ▶ E. Rains, *Efficient computation of isomorphisms between finite fields*, 199x.
- Artin-Schreier towers,  $\ell = p$ :
  - ▶ D. G. Cantor, *On arithmetical algorithms over finite fields*, 1989.
  - ▶ J.-M. Couveignes, *Isomorphisms between Artin-Schreier towers*, 2000.
  - ▶ De Feo and Schost, *Fast arithmetics in Artin-Schreier towers over finite fields*, 2012.
- $\ell$ -adic towers,  $\ell = 2$ :
  - ▶ Doliskani and Schost, *A note on computations in degree  $2^k$ -extensions of finite fields*, 2012.
- Inspiration behind this work:
  - ▶ De Smit and Lenstra, *Standard models for finite fields*, 2008.
  - ▶ Couveignes and Lercier, *Fast construction of irreducible polynomials over finite fields*, 2011.
  - ▶ V. Shoup, *Fast construction of irreducible polynomials over finite fields*, 1994.

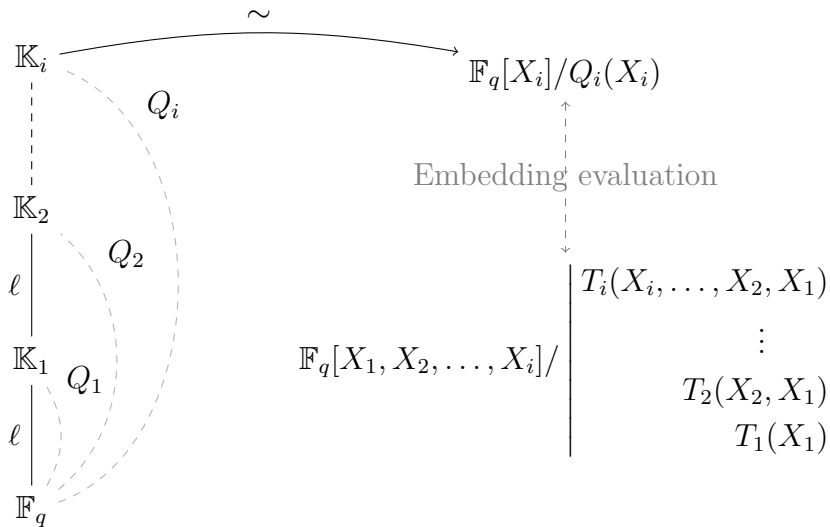
## Univariate vs. Multivariate

$$\begin{array}{c}
 \mathbb{K}_i \\
 \vdots \\
 \mathbb{K}_2 \\
 \ell \mid \\
 \mathbb{K}_1 \\
 \ell \mid \\
 \mathbb{F}_q
 \end{array}
 \qquad
 \mathbb{F}_q[X_1, X_2, \dots, X_i] /
 \begin{array}{c}
 T_i(X_i, \dots, X_2, X_1) \\
 \vdots \\
 T_2(X_2, X_1) \\
 T_1(X_1)
 \end{array}
 \qquad
 \mathbb{F}_q[X_i] / Q_i(X_i)$$

## Univariate vs. Multivariate



## Univariate vs. Multivariate



## Summary of Main Results

### Objective

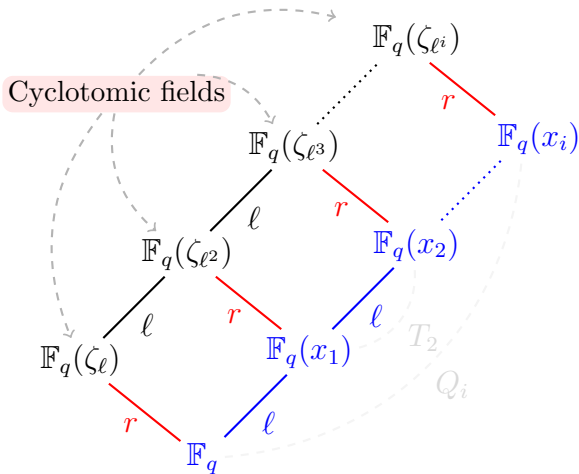
- $q$  and  $\ell$  fixed,
- $\tilde{O}(\ell^i)$  operations in  $\mathbb{F}_q$ ,
- limit additional factors in  $\ell$  and  $q$  as much as possible.

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



## Quasi-cyclotomic towers

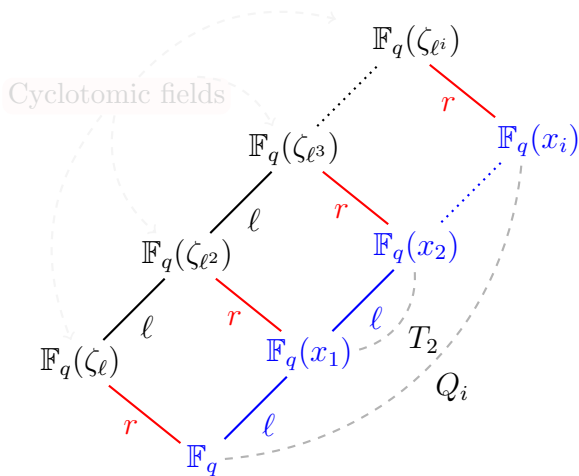
(inspired by Shoup, De Smit and Lenstra)



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

## Quasi-cyclotomic towers

(inspired by Shoup, De Smit and Lenstra)



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

## Quasi-cyclotomic towers

### 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

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

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

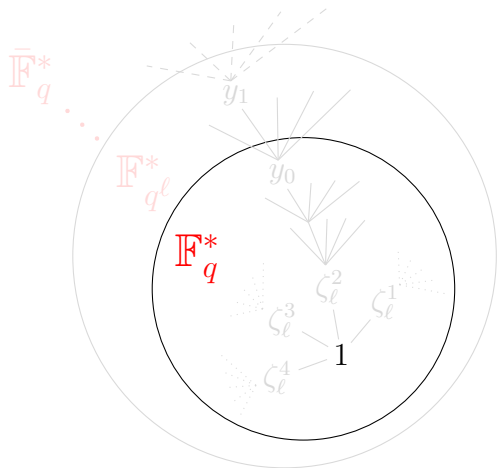
By direct resultant computation

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

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

## Towers from irreducible fibers (Couveignes and Lercier, 2011)

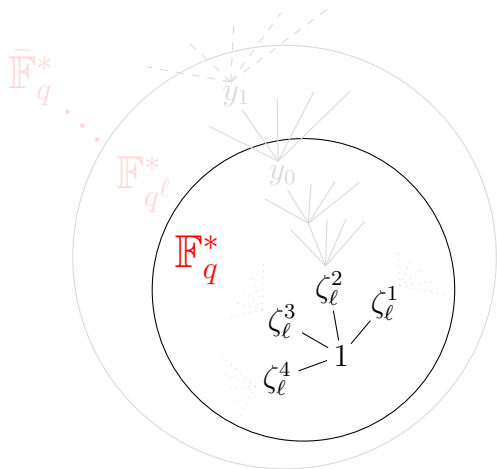
$\ell \mid (q - 1)$ , consider the map  $\phi : x \mapsto x^\ell$



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

## Towers from irreducible fibers (Couveignes and Lercier, 2011)

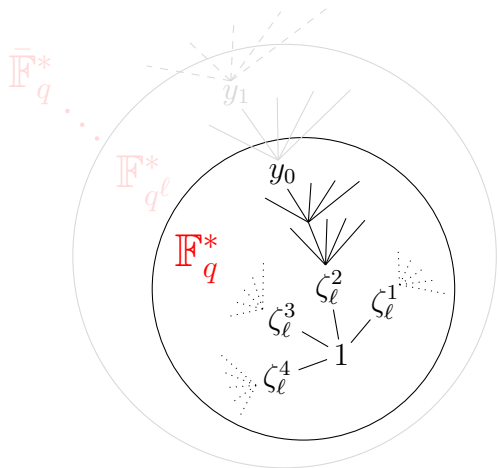
$\ell \mid (q - 1)$ , consider the map  $\phi : x \mapsto x^\ell$



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

## Towers from irreducible fibers (Couveignes and Lercier, 2011)

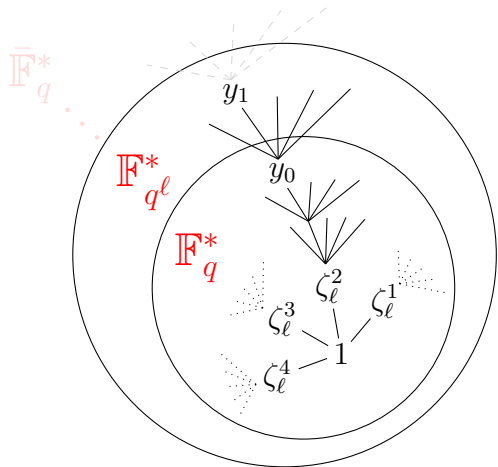
$\ell \mid (q - 1)$ , consider the map  $\phi : x \mapsto x^\ell$



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

## Towers from irreducible fibers (Couveignes and Lercier, 2011)

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

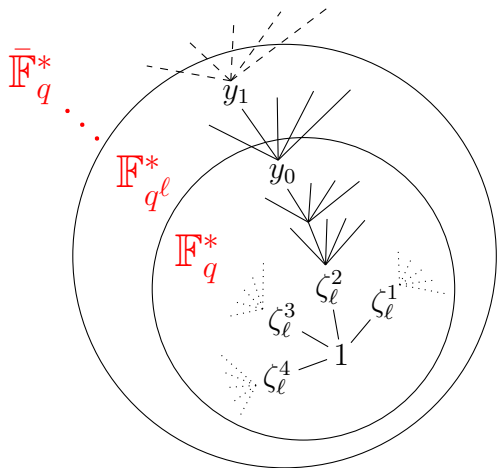


- $\phi|_{\mathbb{F}_q^*}$  not surjective;
- $\phi : \mathbb{G}_m \rightarrow \mathbb{G}_m$  surjective;
- Starting from  $y_0$ , every  $\phi^{-1}y_i$  is an irreducible set of cardinality  $\ell$ .



## Towers from irreducible fibers (Couveignes and Lercier, 2011)

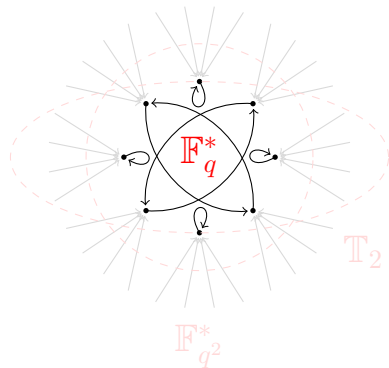
$\ell \mid (q - 1)$ , consider the map  $\phi : x \mapsto x^\ell$



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

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

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

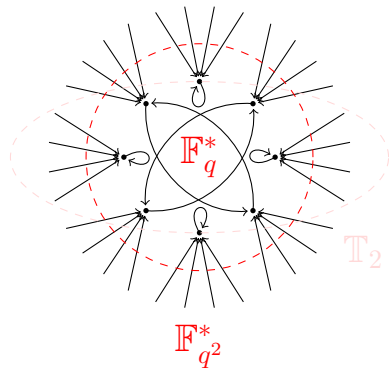


- $\phi|_{\mathbb{F}_q^*}$  bijective;
- $\phi|_{\mathbb{F}_{q^2}^*}$  non surjective;
- $\mathbb{T}_2 \subset \mathbb{F}_{q^2}^*$  algebraic torus of cardinality  $q + 1$ .

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

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

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

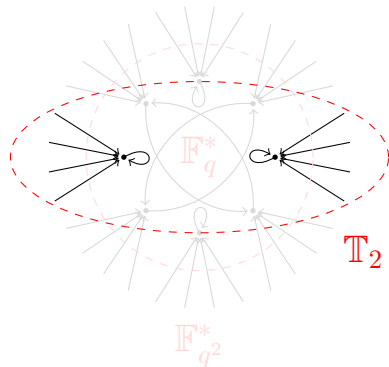


- $\phi|_{\mathbb{F}_q^*}$  bijective;
- $\phi|_{\mathbb{F}_{q^2}^*}$  non surjective;
- $\mathbb{T}_2 \subset \mathbb{F}_{q^2}^*$  algebraic torus of cardinality  $q + 1$ .

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

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

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

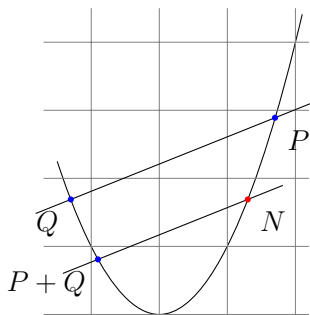


- $\phi|_{\mathbb{F}_q^*}$  bijective;
- $\phi|_{\mathbb{F}_{q^2}^*}$  non surjective;
- $\mathbb{T}_2 \subset \mathbb{F}_{q^2}^*$  algebraic torus of cardinality  $q + 1$ .

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

## Towers from algebraic tori (Pell conics)

- By Weil descent,  $\mathbb{T}_2$  is isomorphic to a *Pell conic*;
- Multiplication in  $\overline{\mathbb{F}}_q$  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

- $\mathbb{T}_2 \rightarrow$  Pell conic  $C$ ,
- multiplication in  $\mathbb{F}_{q^2} \rightarrow$  addition in  $C$ ,
- $\ell$ -th power  $\rightarrow$  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  $\ell C$ , 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

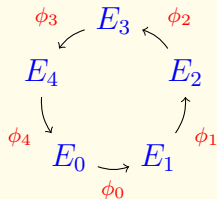
- **Problem 1:** there is essentially one conic; we would like to have more group choices, **elliptic curves** are an option.
- **Problem 2:**  $\ell$ -multiplication on elliptic curves is a degree  $\ell^2$  map; we must consider **separable isogenies** instead.

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

Under these assumptions, isogenies form a cycle

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

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



## Towers from elliptic curves

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  $\ell^{i-j}$ .

## Vélu's formulas

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

## The $\ell$ -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

### 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 $\rightarrow$ Univariate

---

### Algorithm 1 Compose

---

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

```
1: if  $n = 1$  then  
2:   return  $P$   
3: else  
4:    $m \leftarrow \lceil n/2 \rceil$   
5:   Let  $P_0, P_1$  be such that  $P = P_0 + X^m P_1$   
6:    $Q_0 \leftarrow \text{Compose}(P_0, f, g, m)$   
7:    $Q_1 \leftarrow \text{Compose}(P_1, f, g, n - m)$   
8:    $Q \leftarrow Q_0 g^{n-m} + Q_1 f^m$   
9:   return  $Q$   
10: end if
```

---

## Theorem

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

## Pushing: Univariate $\rightarrow$ Multivariate

---

**Algorithm 2** Decompose

---

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

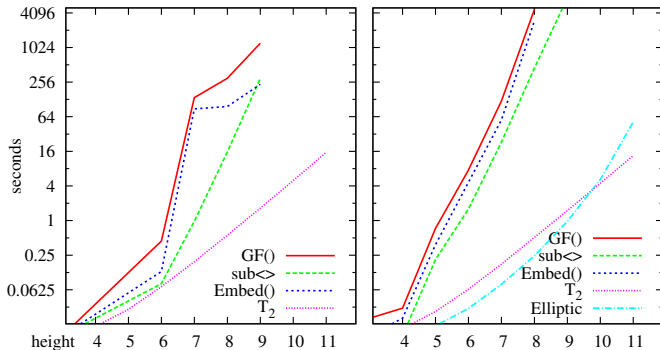
```
1: if  $n = 1$  then  
2:   return  $Q$   
3: else  
4:    $m \leftarrow \lceil n/2 \rceil$   
5:    $u \leftarrow 1/g^{n-m} \bmod f^m$   
6:    $Q_0 \leftarrow Qu \bmod f^m$   
7:    $Q_1 \leftarrow (Q - Q_0g^{n-m}) \operatorname{div} f^m$   
8:    $P_0 \leftarrow \text{Decompose}(Q_0, f, g, h, m)$   
9:    $P_1 \leftarrow \text{Decompose}(Q_1, f, g, h, n - m)$   
10:  return  $P_0 + X^m P_1$   
11: end if
```

---

### Theorem

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