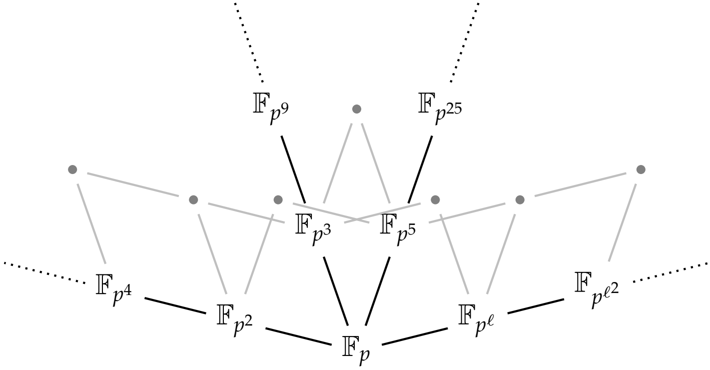
Standard lattices of compatibly embedded finite fields

Luca De Feo, Hugues Randriam, Édouard Rousseau

July 16, 2019

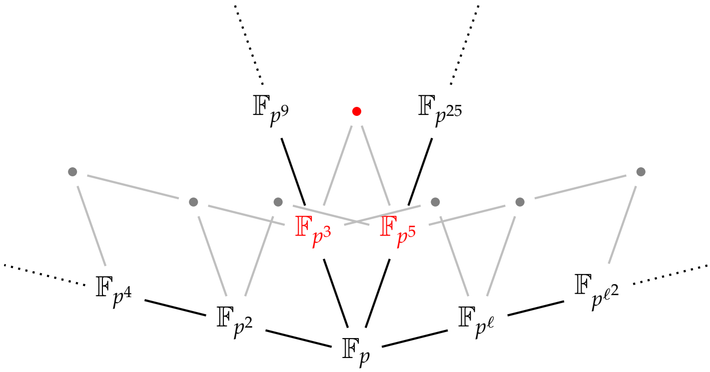
Context

- Use of Computer Algebra System (CAS)
- Use of many extensions of a prime finite field $\mathbb{F}_p$
- Computations in $\bar{\mathbb{F}}_p$.



CONTEXT

- Use of Computer Algebra System (CAS)
- Use of many extensions of a prime finite field $\mathbb{F}_p$
- Computations in $\bar{\mathbb{F}}_p$.



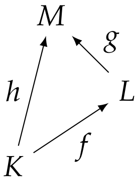
EMBEDDINGS

- When $l \mid m$, we know $\mathbb{F}_{p^l} \hookrightarrow \mathbb{F}_{p^m}$
  - How to compute this embedding *efficiently*?
- Naive algorithm: if $\mathbb{F}_{p^l} = \mathbb{F}_p[x]/(f(x))$, find a root ρ of f in $\mathbb{F}_{p^m}$ and map $\bar{x}$ to ρ. Complexity strictly larger than $\tilde{O}(l^2)$.
- Lots of other solutions in the litterature:
  - [Lenstra '91]
  - [Allombert '02] $\tilde{O}(l^2)$
  - [Rains '96]
  - [Narayanan '18]

Compatibility

- K, L, M three finite fields with $K \hookrightarrow L \hookrightarrow M$
- $f : K \hookrightarrow L$, $g : L \hookrightarrow M$, $h : K \hookrightarrow M$ embeddings

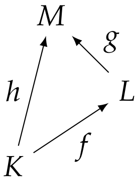
Compatibility:



COMPATIBILITY

- K, L, M three finite fields with $K \hookrightarrow L \hookrightarrow M$
- $f : K \hookrightarrow L$, $g : L \hookrightarrow M$, $h : K \hookrightarrow M$ embeddings

Compatibility:



$$g \circ f \stackrel{?}{=} h$$

Ensuring compatibility: Conway polynomials

Definition (m-th Conway polynomials C_m)

- monic
- irreducible
- degree m
- primitive (*i.e.* its roots generate $\mathbb{F}_{p^m}^\times$)
- *norm-compatible* (*i.e.* $C_l\left(X^{\frac{p^m-1}{p^l-1}} = 0\right) = 0 \mod C_m$ if $l \mid m$)

Ensuring compatibility: Conway polynomials

Definition (m-th Conway polynomials C_m)

- monic
- irreducible
- degree m
- primitive (*i.e.* its roots generate $\mathbb{F}_{p^m}^\times$)
- *norm-compatible* (*i.e.* $C_l\left(X^{\frac{p^m-1}{p^l-1}} = 0\right) = 0 \mod C_m$ if $l \mid m$)

- Standard polynomials

Ensuring compatibility: Conway polynomials

Definition (m-th Conway polynomials C_m)

- monic
- irreducible
- degree m
- primitive (*i.e.* its roots generate $\mathbb{F}_{p^m}^{\times}$)
- *norm-compatible* (*i.e.* $C_l\left(X^{\frac{p^m-1}{p^l-1}}=0\right)=0 \mod C_m$ if $l \mid m$)

- Standard polynomials
- Compatible embeddings: $\bar{X} \mapsto \bar{Y}^{\frac{p^m-1}{p^l-1}}$ $\tilde{O}(m^2)$

Ensuring compatibility: Conway polynomials

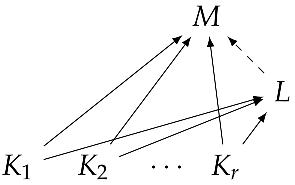
Definition (m-th Conway polynomials C_m)

- monic
- irreducible
- degree m
- primitive (*i.e.* its roots generate $\mathbb{F}_{p^m}^\times$)
- *norm-compatible* (*i.e.* $C_l\left(X^{\frac{p^m-1}{p^l-1}} = 0\right) = 0 \mod C_m$ if $l \mid m$)

- Standard polynomials
- Compatible embeddings: $\bar{X} \mapsto \bar{Y}^{\frac{p^m-1}{p^l-1}}$ $\tilde{O}(m^2)$
- Hard to compute (exponential complexity)

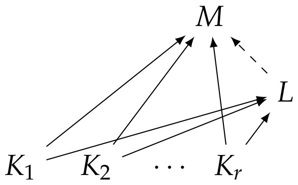
Ensuring compatibility: Bosma, Cannon and Steel

- Framework used in MAGMA
- Based on the naive embedding algorithm
- Constraints on the embedding imply that adding a new embedding can be expensive



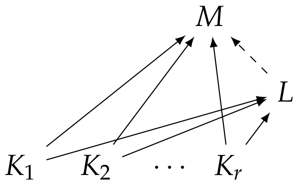
ENSURING COMPATIBILITY: BOSMA, CANNON AND STEEL

- Framework used in MAGMA
- Based on the naive embedding algorithm
- Constraints on the embedding imply that adding a new embedding can be expensive
  - Inefficient as the number of extensions grows



ENSURING COMPATIBILITY: BOSMA, CANNON AND STEEL

- Framework used in MAGMA
- Based on the naive embedding algorithm
- Constraints on the embedding imply that adding a new embedding can be expensive
  - Inefficient as the number of extensions grows



- Non standard polynomials

IDEAS

- Plugging Allombert's embedding algorithm in Bosma, Cannon, and Steel
- Generalizing Bosma, Cannon, and Steel
- Generalizing Conway polynomials

Goal: bring the best of both worlds

ALLOMBERT'S EMBEDDING ALGORITHM I

- Based on *Kummer theory*
- For $l \mid (p-1)$, we work in $\mathbb{F}_{p^l}$, and study

$$\sigma(x) = \zeta_l x \qquad \text{(H90)}$$

where $(\zeta_l)^l = 1$ and $\zeta_l \in \mathbb{F}_p \subset \mathbb{F}_{p^l}$

- Solutions of (H90) form a $\mathbb{F}_p$-vector space of dimension 1
- α_l solution of (H90) generates $\mathbb{F}_{p^l}$
- $(\alpha_l)^l = c \quad \in \mathbb{F}_p$

Allombert's embedding algorithm II

Input: $\mathbb{F}_{p^l}$, $\mathbb{F}_{p^m}$, with $l \mid m \mid (p-1)$, ζ_l and ζ_m with $(\zeta_m)^{m/l} = \zeta_l$
Output: $s \in \mathbb{F}_{p^l}$, $t \in \mathbb{F}_{p^m}$, such that $s \mapsto t$ defines an embedding $\phi : \mathbb{F}_{p^l} \to \mathbb{F}_{p^m}$

1. Find $\alpha_l \in \mathbb{F}_{p^l}$ and $\alpha_m \in \mathbb{F}_{p^m}$, nonzero solutions of (H90) for the roots ζ_l and ζ_m
2. Compute $(\alpha_l)^l = c_l$ and $(\alpha_m)^m = c_m$
3. Compute $\kappa_{l,m}$ a l-th root of c_l/c_m
4. Return α_l and $\kappa_{l,m}(\alpha_m)^{m/l}$

Allombert and Bosma, Canon, and Steel

- Need to store one constant $\kappa_{l,m}$ for each pair $(\mathbb{F}_{p^l}, \mathbb{F}_{p^m})$
- The constant $\kappa_{l,m}$ depends on α_l and α_m

We would like to:

- get rid of the constants $\kappa_{l,m}$ (*e.g.* have $\kappa_{l,m} = 1$)
- equivalently, get "standard" solutions of (H90)
  - select solutions α_l, α_m that always define the same embedding
  - such that the constants $\kappa_{l,m}$ are well understood (*e.g.* $\kappa_{l,m} = 1$)

Can we have $\kappa_{l,m} = 1$?

Let $l \mid m \mid p - 1$, $(\zeta_m)^{m/l} = \zeta_l$

- $\alpha_l \in \mathbb{F}_{p^l}$ and $\alpha_m \in \mathbb{F}_{p^m}$ solutions of H90 for ζ_l and ζ_m
- $\kappa_{l,m} = \sqrt[l]{c_l/c_m} = 1$ implies $c_l = c_m$

Can we have $\kappa_{l,m} = 1$?

Let $l \mid m \mid p-1$, $(\zeta_m)^{m/l} = \zeta_l$

- $\alpha_l \in \mathbb{F}_{p^l}$ and $\alpha_m \in \mathbb{F}_{p^m}$ solutions of H90 for ζ_l and ζ_m
- $\kappa_{l,m} = \sqrt[l]{c_l/c_m} = 1$ implies $c_l = c_m$

In particular, for $m = p-1$

$$\sigma(\alpha_{p-1}) = (\alpha_{p-1})^p = \zeta_{p-1}\alpha_{p-1}$$

Can we have $\kappa_{l,m} = 1$?

Let $l \mid m \mid p-1$, $(\zeta_m)^{m/l} = \zeta_l$

- $\alpha_l \in \mathbb{F}_{p^l}$ and $\alpha_m \in \mathbb{F}_{p^m}$ solutions of H90 for ζ_l and ζ_m
- $\kappa_{l,m} = \sqrt[l]{c_l/c_m} = 1$ implies $c_l = c_m$

In particular, for $m = p-1$

$$\sigma(\alpha_{p-1}) = (\alpha_{p-1})^p = \zeta_{p-1}\alpha_{p-1}$$

- $(\alpha_{p-1})^{p-1} = c_{p-1} = \zeta_{p-1}$

Can we have $\kappa_{l,m} = 1$?

Let $l \mid m \mid p-1$, $(\zeta_m)^{m/l} = \zeta_l$

- $\alpha_l \in \mathbb{F}_{p^l}$ and $\alpha_m \in \mathbb{F}_{p^m}$ solutions of H90 for ζ_l and ζ_m
- $\kappa_{l,m} = \sqrt[l]{c_l/c_m} = 1$ implies $c_l = c_m$

In particular, for $m = p-1$

$$\sigma(\alpha_{p-1}) = (\alpha_{p-1})^p = \zeta_{p-1}\alpha_{p-1}$$

- $(\alpha_{p-1})^{p-1} = c_{p-1} = \zeta_{p-1}$
- this implies $\forall l \mid p-1,\ c_l = \zeta_{p-1}$

Standard solutions

How to define **standard solutions** of (H90)?

Definition (Standard solution)

Let $l \mid p-1$ and $\alpha_l \in \mathbb{F}_{p^l}$ a solution of (H90) for $\zeta_l = (\zeta_{p-1})^{\frac{p-1}{l}}$, α_l is **standard** if $c_l = \zeta_{p-1}$.

Definition (Standard polynomial)

All standard solutions α_l define the same irreducible polynomial of degree l, we call it the **standard polynomial** of degree l.

Standard embeddings

Let $l \mid m \mid p - 1$

- $\zeta_l = (\zeta_m)^{m/l}$
- α_l and α_m **standard solutions** of (H90) for ζ_l and ζ_m

STANDARD EMBEDDINGS

Let $l \mid m \mid p-1$

- $\zeta_l = (\zeta_m)^{m/l}$
- α_l and α_m **standard solutions** of (H90) for ζ_l and ζ_m
  - $c_l = c_m = \zeta_{p-1}$

STANDARD EMBEDDINGS

Let $l \mid m \mid p-1$

- $\zeta_l = (\zeta_m)^{m/l}$
- α_l and α_m **standard solutions** of (H90) for ζ_l and ζ_m
  - $c_l = c_m = \zeta_{p-1}$
    - $\kappa_{l,m} = 1$

STANDARD EMBEDDINGS

Let $l \mid m \mid p-1$

- $\zeta_l = (\zeta_m)^{m/l}$
- α_l and α_m **standard solutions** of (H90) for ζ_l and ζ_m
  - $c_l = c_m = \zeta_{p-1}$
    - $\kappa_{l,m} = 1$
- The embedding $\alpha_l \mapsto (\alpha_m)^{m/l}$ is **standard** too (only depends on ζ_{p-1}).

What happens when $l \nmid p-1$?

Let $p \nmid l$ and $l \nmid p-1$

- no l-th root of unity ζ_l in $\mathbb{F}_p$
  - **add them!** Consider $A_l = \mathbb{F}_{p^l} \otimes \mathbb{F}_p(\zeta_l)$ instead of $\mathbb{F}_{p^l}$

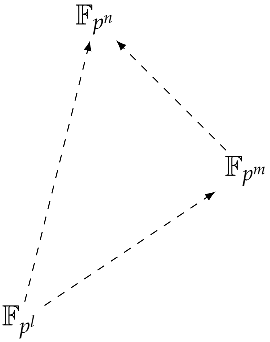
$$(\sigma \otimes 1)(x) = (1 \otimes \zeta_l)x \qquad \text{(H90')}$$

- Allombert's algorithm still works!

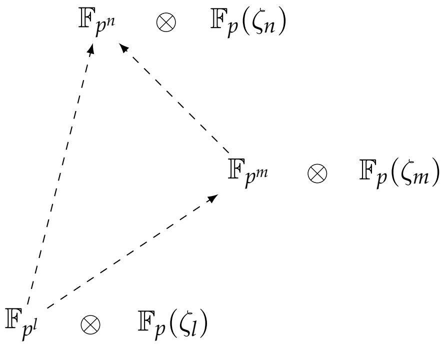
If $l \mid m$ and $(\zeta_m)^{m/l} = \zeta_l$

- Still possible to find **standard solutions** α_l, α_m of H90′
- $\kappa_{l,m} \neq 1$ but easy to compute
- **Standard embedding** from α_l and α_m

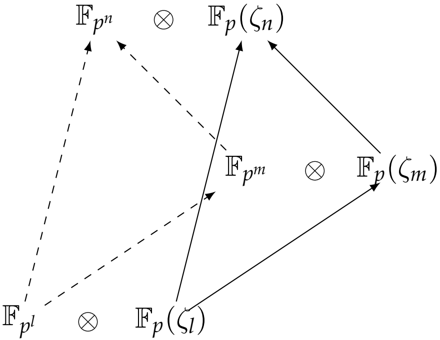
SCHEME OF OUR WORK



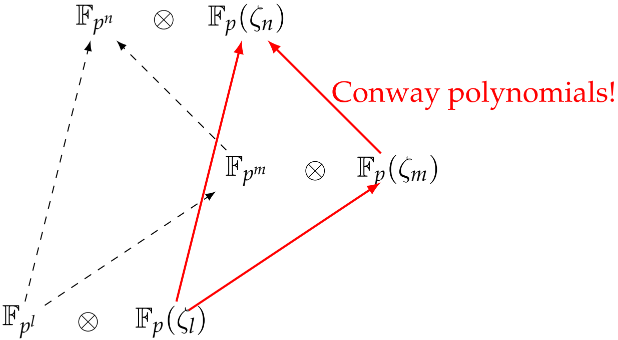
SCHEME OF OUR WORK



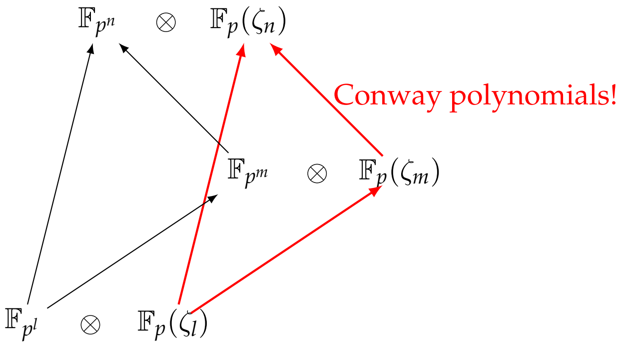
Scheme of our work



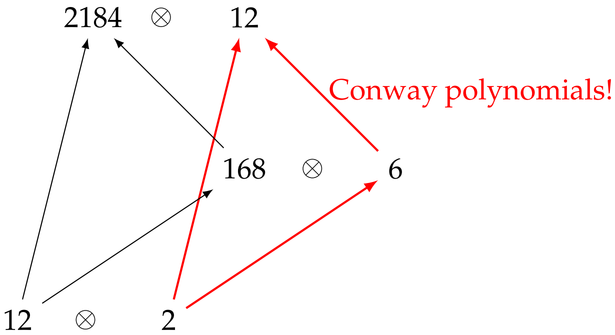
SCHEME OF OUR WORK



SCHEME OF OUR WORK



Scheme of our work



$p = 5$

Compatibility and complexity

Proposition (Compatibility)

Let $l \mid m \mid n$ and $f : \mathbb{F}_{p^l} \hookrightarrow \mathbb{F}_{p^m}$, $g : \mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$, $h : \mathbb{F}_{p^l} \hookrightarrow \mathbb{F}_{p^n}$ the standard embeddings. Then we have $g \circ f = h$.

Proposition (Complexity)

Given a collection of Conway polynomials of degree up to d, for any $l \mid m \mid p^i - 1, i \leq d$

- *Computing a standard solution α_l takes $\tilde{O}(l^2)$*
- *Given α_l and α_m, computing the standard embedding $f : \mathbb{F}_{p^l} \hookrightarrow \mathbb{F}_{p^m}$ takes $\tilde{O}(m^2)$*

Implementation

Implementation using Flint/C and Nemo/Julia.

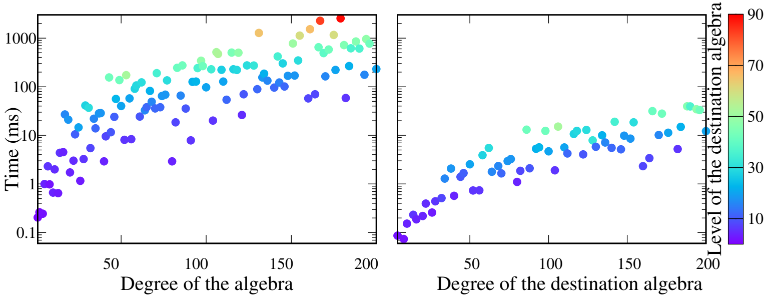


Figure: Timings for computing α_l (left, logscale), and for computing $\mathbb{F}_{p^2} \hookrightarrow \mathbb{F}_{p^l}$ (right, logscale) for $p = 3$.

Standard polynomials

$$x + 1$$
$$x^3 + x + 1$$
$$x^5 + x^3 + 1$$
$$x^7 + x + 1$$
$$x^9 + x^7 + x^4 + x^2 + 1$$
$$x^{11} + x^8 + x^7 + x^6 + x^2 + x + 1$$
$$x^{13} + x^{10} + x^5 + x^3 + 1$$
$$x^{15} + x + 1$$
$$x^{17} + x^{11} + x^{10} + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1$$
$$x^{19} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^8 + x^7 + x^6 + x^5 + x^3 + 1$$

Table: The ten first standard polynomials derived from Conway polynomials for $p = 2$.

Conclusion, open problems

- We implicitly assume that we have **compatible roots** ζ (*i.e.* $\zeta_l = (\zeta_m)^{m/l}$ for $l \mid m$)
  - In practice, this is done using **Conway polynomials**
- With Conway polynomials up to degree d, we can compute embeddings to finite fields up to any degree $l \mid p^i - 1, i \leq d$
  - quasi-quadratic complexity

Open problems:

- Make this work less standard, but more practical
- Can we prove better than quasi-quadratic?
  - for the isomorphism problem (in the general case)
  - for the computations in $\bar{\mathbb{F}}_p$
- Compute (pseudo-)Conway polynomials faster

Thank you!