Standard lattices of compatibly embedded finite fields

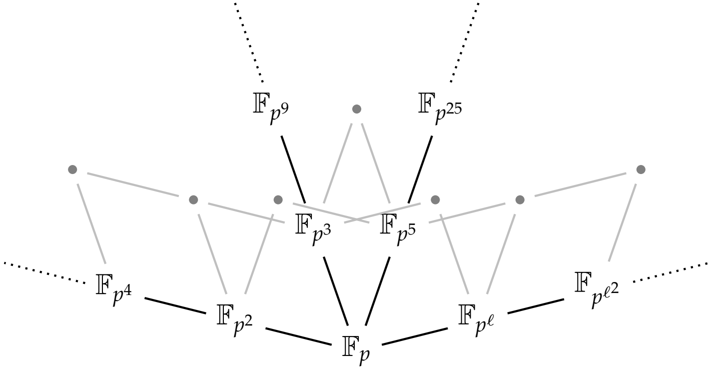
Luca De Feo, Hugues Randriam, Édouard Rousseau

JNCF 2019

CONTENTS

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:

$$\begin{tikzcd} M & \\ & L \arrow[ul, "g"'] \\ K \arrow[uu, "h"] \arrow[ur, "f"'] & \end{tikzcd}$$

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:

$$\begin{tikzcd} M & \\ & L \arrow[ul, "g"'] \\ K \arrow[uu, "h"] \arrow[ur, "f"'] & \end{tikzcd}$$

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

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

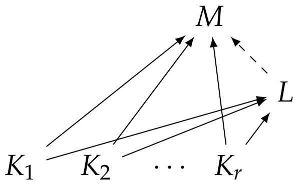
Definition (m-th Conway polynomials C_m)

- 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)

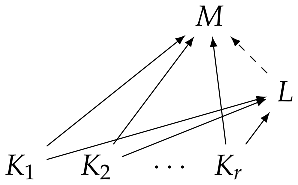
Ensuring compatibility: Bosma, Cannon and Steel

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



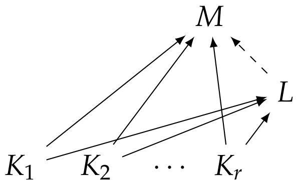
Ensuring compatibility: Bosma, Cannon and Steel

- Framework used in MAGMA
- Based on the naive embedding algorithm
- Constraints of 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 of 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 an extension of *Kummer theory*
- For $p \nmid l$, we work in $A_l = \mathbb{F}_{p^l} \otimes \mathbb{F}_p(\zeta_l)$, and study

$$(\sigma \otimes 1)(x) = (1 \otimes \zeta_l)x \tag{H90}$$

- Solutions of (H90) form a $\mathbb{F}_p(\zeta_l)$-vector space of dimension 1
- $\alpha_l = \sum_{j=0}^{a-1} x_j \otimes \zeta_l^j$ solution of (H90), then x_0 generates $\mathbb{F}_{p^l}$.
  - Let $\lfloor \alpha_l \rfloor = x_0$ the projection on the first coordinate
- $(\alpha_l)^l = 1 \otimes c \quad \in 1 \otimes \mathbb{F}_p(\zeta_l)$

ALLOMBERT'S EMBEDDING ALGORITHM II

Input: $\mathbb{F}_{p^l}$, $\mathbb{F}_{p^m}$, with $l \mid m$, 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. Construct A_l and A_m
2. Find $\alpha_l \in A_l$ and $\alpha_m \in A_m$, nonzero solutions of (H90) for the roots ζ_l and ζ_m
3. Compute $(\alpha_l)^l = 1 \otimes c_l$ and $(\alpha_m)^m = 1 \otimes c_m$
4. Compute $\kappa_{l,m}$ a l-th root of c_l/c_m
5. Return $\lfloor \alpha_l \rfloor$ and $\left\lfloor (1 \otimes \kappa_{l,m})(\alpha_m)^{m/l} \right\rfloor$

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.* $\kappa_{l,m} = 1$)

THE CASE $l \mid m \mid p-1$

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

- $A_l = \mathbb{F}_{p^l} \otimes \mathbb{F}_p \cong \mathbb{F}_{p^l}$
- $A_m = \mathbb{F}_{p^m}$
- $\sigma(\alpha_l) = \zeta_l \alpha_l$ and $\sigma(\alpha_m) = \zeta_m \alpha_m$
- $(\alpha_l)^l = c_l \quad \in \mathbb{F}_p$ and $(\alpha_m)^m = c_m \quad \in \mathbb{F}_p$
- $\kappa_{l,m} = \sqrt[l]{c_l/c_m}$
- $\kappa_{l,m} = 1$ implies $c_l = c_m$

In particular, for $m = p-1$ we obtain
$\sigma(\alpha_{p-1}) = (\alpha_{p-1})^p = \zeta_{p-1}\alpha_{p-1}$

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

Complete algebra

Let $A_l = \mathbb{F}_{p^l} \otimes \mathbb{F}_p(\zeta_l)$

Definition (degree, level)

- *degree* of A_l: l
- *level* of A_l: $a = [\mathbb{F}_p(\zeta_l) : \mathbb{F}_p]$

Idea: consider the largest algebra for a given level

Definition (Complete algebra of level a)

- $A_{p^a-1} = \mathbb{F}_{p^{p^a-1}} \otimes \mathbb{F}_p(\zeta_{p^a-1}) \cong \mathbb{F}_{p^{p^a-1}} \otimes \mathbb{F}_{p^a}$

STANDARD SOLUTIONS

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

Lemma

If α_{p^a-1} *is a solution of* (H90) *for* ζ_{p^a-1}*, then* $c_{p^a-1} = (\zeta_{p^a-1})^a$*.*

Definition (Standard solution)

Let A_l an algebra of level a, $\alpha_l \in A_l$ a solution of (H90) for $\zeta_l = (\zeta_{p^a-1})^{\frac{p^a-1}{l}}$, α_l is **standard** if $c_l = (\zeta_{p^a-1})^a$

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 (same level)

Let $l \mid m$ and A_l, A_m algebras with the **same level** a, $\zeta_l = (\zeta_m)^{m/l}$

- α_l and α_m **standard** solutions of (H90) for ζ_l and ζ_m

Standard embeddings (same level)

Let $l \mid m$ and A_l, A_m algebras with the **same level** a, $\zeta_l = (\zeta_m)^{m/l}$

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

Standard embeddings (same level)

Let $l \mid m$ and A_l, A_m algebras with the **same level** a, $\zeta_l = (\zeta_m)^{m/l}$

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

Standard embeddings (same level)

Let $l \mid m$ and A_l, A_m algebras with the **same level** a, $\zeta_l = (\zeta_m)^{m/l}$

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

STANDARD EMBEDDINGS (DIFFERENT LEVEL)

Let $l \mid m$ and A_l of level a, A_m of level b, $a \neq b$.

- Natural norm-compatibility condition, we want:

$$(\zeta_{p^b-1})^{\frac{p^b-1}{p^a-1}} = N(\zeta_{p^b-1}) = \phi_{\mathbb{F}_{p^a} \hookrightarrow \mathbb{F}_{p^b}}(\zeta_{p^a-1})$$

Standard embeddings (different level)

Let $l \mid m$ and A_l of level a, A_m of level b, $a \neq b$.

- Natural norm-compatibility condition, we want:

$$(\zeta_{p^b-1})^{\frac{p^b-1}{p^a-1}} = N(\zeta_{p^b-1}) = \phi_{\mathbb{F}_{p^a} \hookrightarrow \mathbb{F}_{p^b}}(\zeta_{p^a-1})$$

We let $\mathcal{N}$ be the "norm-like" map $\mathcal{N}(\alpha) = \prod_{j=0}^{b/a-1}(1 \otimes \sigma^{aj})(\alpha)$

Standard embeddings (different level)

Let $l \mid m$ and A_l of level a, A_m of level b, $a \neq b$.

- Natural norm-compatibility condition, we want:

$$(\zeta_{p^b-1})^{\frac{p^b-1}{p^a-1}} = N(\zeta_{p^b-1}) = \phi_{\mathbb{F}_{p^a} \hookrightarrow \mathbb{F}_{p^b}}(\zeta_{p^a-1})$$

We let $\mathcal{N}$ be the "norm-like" map $\mathcal{N}(\alpha) = \prod_{j=0}^{b/a-1}(1 \otimes \sigma^{aj})(\alpha)$

- We obtain $\mathcal{N}(\alpha_{p^b-1}) = \Phi_{A_{p^a-1} \hookrightarrow A_{p^b-1}}(\alpha_{p^a-1})$

Standard embeddings (different level)

Let $l \mid m$ and A_l of level a, A_m of level b, $a \neq b$.

- Natural norm-compatibility condition, we want:

$$(\zeta_{p^b-1})^{\frac{p^b-1}{p^a-1}} = N(\zeta_{p^b-1}) = \phi_{\mathbb{F}_{p^a} \hookrightarrow \mathbb{F}_{p^b}}(\zeta_{p^a-1})$$

We let $\mathcal{N}$ be the "norm-like" map $\mathcal{N}(\alpha) = \prod_{j=0}^{b/a-1}(1 \otimes \sigma^{aj})(\alpha)$

- We obtain $\mathcal{N}(\alpha_{p^b-1}) = \Phi_{A_{p^a-1} \hookrightarrow A_{p^b-1}}(\alpha_{p^a-1})$
- We know that $(\alpha_{p^b-1})^{\frac{p^b-1}{p^a-1}} = (1 \otimes \kappa_{p^a-1,p^b-1})\Phi_{A_{p^a-1} \hookrightarrow A_{p^b-1}}(\alpha_{p^a-1})$ with $\kappa_{p^a-1,p^b-1} = (\zeta_{p^b-1})^{\frac{(a-b)p^{a+b}+bp^b-ap^a}{(p^a-1)^2}}$

Standard embeddings (different level)

Let $l \mid m$ and A_l of level a, A_m of level b, $a \neq b$.

- Natural norm-compatibility condition, we want:

$$(\zeta_{p^b-1})^{\frac{p^b-1}{p^a-1}} = N(\zeta_{p^b-1}) = \phi_{\mathbb{F}_{p^a} \hookrightarrow \mathbb{F}_{p^b}}(\zeta_{p^a-1})$$

We let $\mathcal{N}$ be the "norm-like" map $\mathcal{N}(\alpha) = \prod_{j=0}^{b/a-1}(1 \otimes \sigma^{aj})(\alpha)$

- We obtain $\mathcal{N}(\alpha_{p^b-1}) = \Phi_{A_{p^a-1} \hookrightarrow A_{p^b-1}}(\alpha_{p^a-1})$
- We know that $(\alpha_{p^b-1})^{\frac{p^b-1}{p^a-1}} = (1 \otimes \kappa_{p^a-1,p^b-1})\Phi_{A_{p^a-1} \hookrightarrow A_{p^b-1}}(\alpha_{p^a-1})$ with $\kappa_{p^a-1,p^b-1} = (\zeta_{p^b-1})^{\frac{(a-b)p^{a+b}+bp^b-ap^a}{(p^a-1)^2}}$
- If α_l and α_m are **standard solutions**, then $\kappa_{l,m} = (\zeta_{p^b-1})^{\frac{(a-b)p^{a+b}+bp^b-ap^a}{(p^a-1)l}}$

Standard embeddings (different level)

Let $l \mid m$ and A_l of level a, A_m of level b, $a \neq b$ and

- $(\zeta_{p^b-1})^{\frac{p^b-1}{p^a-1}} = N(\zeta_{p^b-1}) = \phi_{\mathbb{F}_{p^a} \hookrightarrow \mathbb{F}_{p^b}}(\zeta_{p^a-1})$
- $\zeta_l = (\zeta_{p^a-1})^{\frac{p^a-1}{l}}$
- $\zeta_m = (\zeta_{p^b-1})^{\frac{p^b-1}{m}}$
- α_l and α_m **standard solutions** of (H90) for ζ_l and ζ_m
- $\kappa_{l,m}$ only depends on ζ_{p^b-1} and **is easy to compute**
- The embedding $\lfloor \alpha_l \rfloor \mapsto \left\lfloor (1 \otimes \kappa_{l,m})(\alpha_m)^{m/l} \right\rfloor$ is **standard** too (only depends on $\zeta_{p^a-1}, \zeta_{p^b-1}$).

STANDARD EMBEDDINGS (DIFFERENT LEVEL)

Let $l \mid m$ and A_l of level a, A_m of level b, $a \neq b$ and

- $(\zeta_{p^b-1})^{\frac{p^b-1}{p^a-1}} = N(\zeta_{p^b-1}) = \phi_{\mathbb{F}_{p^a} \hookrightarrow \mathbb{F}_{p^b}}(\zeta_{p^a-1})$
- $\zeta_l = (\zeta_{p^a-1})^{\frac{p^a-1}{l}}$
- $\zeta_m = (\zeta_{p^b-1})^{\frac{p^b-1}{m}}$
- α_l and α_m **standard solutions** of (H90) for ζ_l and ζ_m
- $\kappa_{l,m}$ only depends on ζ_{p^b-1} and **is easy to compute**
- The embedding $\lfloor \alpha_l \rfloor \mapsto \left\lfloor (1 \otimes \kappa_{l,m})(\alpha_m)^{m/l} \right\rfloor$ is **standard** too (only depends on $\zeta_{p^a-1}, \zeta_{p^b-1}$).

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.

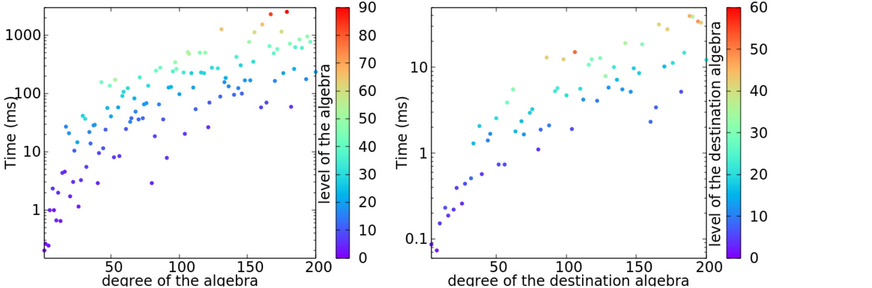


Figure: Timings for computing α_l (left, logscale), and for computing $\mathbb{F}_{p^2} \hookrightarrow \mathbb{F}_{p^l}$ (right, logscale) for $p = 3$.

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, FUTURE WORKS

- 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

Future works:

- Make this less standard, but more practical

Thank you!
Merci !