Lattices of compatibly embedded finite fields

Edouard Rousseau

GT BAC
December 14, 2017

CONTENTS

The embedding problem

The embedding problem

- f irreducible polynomial of degree m in $\mathbb{F}_p[X]$
- g irreducible polynomial of degree n in $\mathbb{F}_p[Y]$
- $m \mid n$
- $E = \mathbb{F}_p[X]/(f(X))$
- $F = \mathbb{F}_p[Y]/(g(Y))$

$$E \cong \mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n} \cong F$$

- **Embedding problem:** how to compute the embedding from E to F ?

Description and evaluation

Two steps:

- Description: find α_1, α_2 such that
  - $E = \mathbb{F}_p(\alpha_1)$
  - *there exists* an embedding $\phi : E \to F$ mapping $\alpha_1 \mapsto \alpha_2$
- Evaluation
  - Compute $\phi(\gamma) \in F$ for $\gamma \in E$
  - Test if $\delta \in \phi(E)$ for $\delta \in F$
  - If $\delta \in \phi(E)$, compute $\phi^{-1}(\delta) \in E$

Description - Naive algorithm

Context:

$$E = \mathbb{F}_p[X]/(f) \qquad F = \mathbb{F}_p[Y]/(g)$$

Algorithm:

- Find a root ρ of f in F
- $\alpha_1 = \overline{X}$
- $\alpha_2 = \rho$

Description - Allombert's algorithm ($m \mid p-1$)

Assume $m \mid p-1$.

- $\exists \zeta \in \mathbb{F}_p$, primitive m-th root of unity
- Find such a ζ
- Solve $\sigma(x) = \zeta x$ in E, where $\sigma :=$ Frobenius automorphism (Hilbert 90)
  - Denote by α_1 a solution
- Solve $\sigma(y) = \zeta y$ in F
  - Denote by α_2 a solution

Facts:

- $E = \mathbb{F}_p(\alpha_1)$
- $a_1 := \alpha_1^m \in \mathbb{F}_p$, $a_2 := \alpha_2^m \in \mathbb{F}_p$
- a_1/a_2 is a m-th power in $\mathbb{F}_p$
  - Compute $c \in \mathbb{F}_p$ such that $c^m = a_1/a_2$

Take the map $\alpha_1 \mapsto c\alpha_2$

Description - Allombert's algorithm

In general:

- We do not necessarily have primitive m-th roots of unity ζ in $\mathbb{F}_p$
- We work in $E \otimes_{\mathbb{F}_p} C$ and $F \otimes_{\mathbb{F}_p} C$, where C is a finite extension of $\mathbb{F}_p$ containing primitive m-th roots of unity
- We use the same kind of results to find α_1, α_2

The compatibility problem

The compatibility problem

Context:

- E, F, G fields
- E subfield of F and F subfield of G
- $\phi_{E\hookrightarrow F}, \phi_{F\hookrightarrow G}, \phi_{E\hookrightarrow G}$ embeddings

$$\begin{tikzcd}
G & \\
& F \arrow[ul, "\phi_{F\hookrightarrow G}"'] \\
E \arrow[uu, "\phi_{E\hookrightarrow G}"] \arrow[ur, "\phi_{E\hookrightarrow F}"'] &
\end{tikzcd}$$

$$\phi_{F\hookrightarrow G} \circ \phi_{E\hookrightarrow F} \stackrel{?}{=} \phi_{E\hookrightarrow G}$$

THE COMPATIBILITY PROBLEM II

$$
\begin{tikzcd}
& H & \\
G \arrow[ur, "\phi_{G\hookrightarrow H}"] & & F \arrow[ul, "\phi_{F\hookrightarrow G}"'] \\
& E \arrow[ul, "\phi_{E\hookrightarrow G}"] \arrow[ur, "\phi_{E\hookrightarrow F}"'] &
\end{tikzcd}
$$

$$\phi_{G\hookrightarrow H} \circ \phi_{E\hookrightarrow G} \stackrel{?}{=} \phi_{F\hookrightarrow H} \circ \phi_{E\hookrightarrow F}$$

Bosma, Cannon and Steel

- Allows to work with arbitrary, user-defined finite fields
- Allows to build the embeddings in arbitrary order
- Used in MAGMA

Bosma, Cannon and Steel framework (theory)

First example

$$\begin{tikzcd}
 & G & \\
 & & F \arrow[ul, dashed] \\
 & E \arrow[uu, "\phi_{E\hookrightarrow G}"] \arrow[ur, "\phi_{E\hookrightarrow F}"'] &
\end{tikzcd}$$

- Take $\phi'_{F\hookrightarrow G}$ an arbitrary embedding between F and G
- Find $\sigma \in \mathrm{Gal}(G/\mathbb{F}_p)$ such that $\sigma \circ \phi'_{F\hookrightarrow G} \circ \phi_{E\hookrightarrow F} = \phi_{E\hookrightarrow G}$
- Set $\phi_{F\hookrightarrow G} := \sigma \circ \phi'_{F\hookrightarrow G}$
- There are $|\mathrm{Gal}(F/E)|$ compatible morphisms

Bosma, Cannon and Steel framework (theory)

What about several subfields $E_1, E_2, \dots, E_r$?

- We impose some conditions on the lattice

  CE1 (Unicity) At most one morphism $\phi_{E \hookrightarrow F}$

  CE2 (Reflexivity) For each E, $\phi_{E \hookrightarrow E} = \mathrm{Id}_E$

  CE3 (Invertibility) For each pair (E, F) with $E \cong F$, $\phi_{E \hookrightarrow F} = \phi^{-1}_{F \hookrightarrow E}$

  CE4 (Transitivity) For any triple (E, F, G) with E subfield of F and F subfield of G, if we have computed $\phi_{E \hookrightarrow F}$ and $\phi_{F \hookrightarrow G}$, then $\phi_{E \hookrightarrow G} = \phi_{F \hookrightarrow G} \circ \phi_{E \hookrightarrow F}$

  CE5 (Intersections) For any triple (E, F, G) with E and F subfields of G, we have that the field $S = E \cap F$ is embedded in E and F, *i.e.* we have computed $\phi_{S \hookrightarrow E}$ and $\phi_{S \hookrightarrow F}$

Bosma, Cannon and Steel framework (theory)

$$\begin{tikzcd}
 & & & G & \\
 & & & & F \arrow[ul, dashed] \\
E_1 \arrow[uurrr] \arrow[urrrr] & E_2 \arrow[uurr] \arrow[urrr] & \cdots & E_r \arrow[uu] \arrow[ur] &
\end{tikzcd}$$

- Set F' the field generated by the fields E_i in F
- Set G' the field generated by the fields E_i in G

Theorem

There exists a unique isomorphism $\chi : F' \to G'$ that is compatible with all embeddings, i.e. such that for all i, $\phi_{E_i \hookrightarrow G'} = \chi \circ \phi_{E_i \hookrightarrow F'}$.

Bosma, Cannon and Steel framework (theory)

$$
\begin{tikzcd}
 & & G & \\
 & & & F \arrow[ul, dashed] \\
G' \arrow[uurr, "\phi_{G' \hookrightarrow G}"] & & F' \arrow[ll, "\chi"'] \arrow[ur, "\phi_{F' \hookrightarrow F}"'] &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
G & \\
 & F \arrow[ul, dashed] \\
F' \arrow[uu, "\phi_{F' \hookrightarrow G}"] \arrow[ur, "\phi_{F' \hookrightarrow F}"'] &
\end{tikzcd}
$$

- We have $|\operatorname{Gal}(F/F')|$ compatible morphisms

Bosma, Cannon and Steel framework (practice)

- Use the naive embedding algorithm

$$\begin{tikzcd}
 & G & \\
 & & F \arrow[lu, dashed] \\
 & E \arrow[uu, "\phi_{E\hookrightarrow G}"] \arrow[ru, "\phi_{E\hookrightarrow F}"'] &
\end{tikzcd}$$

- Consider α such that $F = \mathbb{F}_p(\alpha)$
- Take ρ a root of $\phi_{E\hookrightarrow G}(\mathrm{Minpoly}_E(\alpha))$
- Map $\alpha \mapsto \rho$ and

$$\phi_{F\hookrightarrow G}\Big(\sum_{i=0}^{[F:E]-1} e_i\alpha^i\Big) = \sum_{i=0}^{[F:E]-1} \phi_{E\hookrightarrow G}(e_i)\rho^i$$

Bosma, Cannon and Steel framework (practice)

$$
\begin{tikzcd}
 & & & G & \\
 & & & & F \arrow[ul, dashed] \\
E_1 \arrow[uurrr] \arrow[urrrr] & E_2 \arrow[uurr] \arrow[urrr] & \cdots & E_r \arrow[uu] \arrow[ur] &
\end{tikzcd}
$$

- Consider α such that $F = \mathbb{F}_p(\alpha)$
- Take ρ a root of $\gcd_i(\phi_{E_i \hookrightarrow G}(\mathrm{Minpoly}_{E_i}(\alpha)))$
- Map $\alpha \mapsto \rho$

Bosma, Cannon and Steel framework

To embed F in G:

1. For each subfield S of G, if $S \cap F$ is not embedded in S and F, if not, embed it
2. embed F in G using the method seen before
3. take the transitive closure

Bosma, Cannon and Steel framework

Some configurations with triangles:

$$\begin{tikzcd}
& G & \\
& & F \arrow[ul, dashed] \\
E \arrow[uur] \arrow[urr] & &
\end{tikzcd}
\qquad
\begin{tikzcd}
& G & \\
& & F \arrow[ul] \\
E \arrow[uur, dashed] \arrow[urr] & &
\end{tikzcd}
\qquad
\begin{tikzcd}
& G & \\
& & F \arrow[ul] \\
E \arrow[uur] \arrow[urr, dashed] & &
\end{tikzcd}$$

BOSMA, CANNON AND STEEL FRAMEWORK

Some configurations with triangles:

$$\begin{tikzcd} & G & \\ & & F \arrow[ul, dashed] \\ E \arrow[uur] \arrow[urr] & & \end{tikzcd} \qquad \begin{tikzcd} & G & \\ & & F \arrow[ul] \\ E \arrow[uur, dashed] \arrow[urr] & & \end{tikzcd} \qquad \begin{tikzcd} & G & \\ & & F \arrow[ul] \\ E \arrow[uur] \arrow[urr, dashed] & & \end{tikzcd}$$

$$\begin{tikzcd} & G & \\ & & F \arrow[ul, dashed] \\ E \arrow[uur] & & \end{tikzcd} \qquad \begin{tikzcd} & G & \\ & & F \arrow[ul] \\ E \arrow[uur, dashed] & & \end{tikzcd}$$

Bosma, Cannon and Steel framework

An example of what can happen with the intersections:

$$
\begin{tikzcd}
 & & & \mathbb{F}_{p^{120}} & \\
 & & \mathbb{F}_{p^{60}} \arrow[ur, dashed] & & \mathbb{F}_{p^{40}} \arrow[ul] \\
 & \mathbb{F}_{p^{30}} \arrow[ur] & & & \\
\mathbb{F}_{p^{6}} \arrow[ur] & & & &
\end{tikzcd}
$$

Bosma, Cannon and Steel framework

An example of what can happen with the intersections:

$$
\begin{tikzcd}
 & & & \mathbb{F}_{p^{120}} & \\
 & & \mathbb{F}_{p^{60}} \arrow[ur, dashed] & & \mathbb{F}_{p^{40}} \arrow[ul] \\
 & \mathbb{F}_{p^{30}} \arrow[ur] & & \mathbb{F}_{p^{20}} \arrow[ul, dashed] \arrow[ur] & \\
\mathbb{F}_{p^{6}} \arrow[ur] & & & &
\end{tikzcd}
$$

Bosma, Cannon and Steel framework

An example of what can happen with the intersections:

$$
\begin{tikzcd}
 & & & \mathbb{F}_{p^{120}} & \\
 & & \mathbb{F}_{p^{60}} \arrow[ur, dashed] & & \mathbb{F}_{p^{40}} \arrow[ul] \\
 & \mathbb{F}_{p^{30}} \arrow[ur] & & \mathbb{F}_{p^{20}} \arrow[ul, dashed] \arrow[ur] & \\
\mathbb{F}_{p^{6}} \arrow[ur] & & \mathbb{F}_{p^{10}} \arrow[ul, dashed] \arrow[ur] & &
\end{tikzcd}
$$

Bosma, Cannon and Steel framework

An example of what can happen with the intersections:

$$\begin{tikzcd}
 & & & \mathbb{F}_{p^{120}} & \\
 & & \mathbb{F}_{p^{60}} \arrow[ur, dashed] & & \mathbb{F}_{p^{40}} \arrow[ul] \\
 & \mathbb{F}_{p^{30}} \arrow[ur] & & \mathbb{F}_{p^{20}} \arrow[ul, dashed] \arrow[ur] & \\
\mathbb{F}_{p^{6}} \arrow[ur] & & \mathbb{F}_{p^{10}} \arrow[ul, dashed] \arrow[ur] & & \\
 & \mathbb{F}_{p^{2}} \arrow[ul] \arrow[ur] & & &
\end{tikzcd}$$

Bosma, Cannon and Steel framework

An example of what can happen with the intersections:

$$
\begin{tikzcd}
 & & & \mathbb{F}_{p^{120}} & \\
 & & \mathbb{F}_{p^{60}} \arrow[ur, dashed] & & \mathbb{F}_{p^{40}} \arrow[ul] \\
 & \mathbb{F}_{p^{30}} \arrow[ur] & & \mathbb{F}_{p^{20}} \arrow[ul, dashed] \arrow[ur] & \\
\mathbb{F}_{p^{6}} \arrow[ur] & & \mathbb{F}_{p^{10}} \arrow[ul] \arrow[ur] & & \\
 & \mathbb{F}_{p^{2}} \arrow[ul] \arrow[ur] & & &
\end{tikzcd}
$$

Bosma, Cannon and Steel framework

An example of what can happen with the intersections:

$$
\begin{tikzcd}
 & & & \mathbb{F}_{p^{120}} & \\
 & & \mathbb{F}_{p^{60}} \arrow[ur, dashed] & & \mathbb{F}_{p^{40}} \arrow[ul] \\
 & \mathbb{F}_{p^{30}} \arrow[ur] & & \mathbb{F}_{p^{20}} \arrow[ul] \arrow[ur] & \\
\mathbb{F}_{p^{6}} \arrow[ur] & & \mathbb{F}_{p^{10}} \arrow[ul] \arrow[ur] & & \\
 & \mathbb{F}_{p^{2}} \arrow[ul] \arrow[ur] & & &
\end{tikzcd}
$$

Bosma, Cannon and Steel framework

An example of what can happen with the intersections:

$$
\begin{tikzcd}
 & & & \mathbb{F}_{p^{120}} & \\
 & & \mathbb{F}_{p^{60}} \arrow[ur] & & \mathbb{F}_{p^{40}} \arrow[ul] \\
 & \mathbb{F}_{p^{30}} \arrow[ur] & & \mathbb{F}_{p^{20}} \arrow[ul] \arrow[ur] & \\
\mathbb{F}_{p^{6}} \arrow[ur] & & \mathbb{F}_{p^{10}} \arrow[ul] \arrow[ur] & & \\
 & \mathbb{F}_{p^{2}} \arrow[ul] \arrow[ur] & & &
\end{tikzcd}
$$

Computing an isomorphism with a common subfield

- We want to embed E in F
  - additionnal information: S is a field embedded in E and F
- We factor a degree $[E : S]$ polynomial in F, instead of a degree $[E : \mathbb{F}_p]$ polynomial in F.
- Several common subfields $S_1, S_2, \ldots, S_r$ are equivalent to the field S' generated by the S_i in E

Some questions

- Can we use Bosma, Cannon and Steel framework with a more efficient algorithm ? (*e.g.* Allombert's)
- Can we use a similar common subfield trick with Allombert's algorithm ?

Thank you for your attention !