

# Lattices of compatibly embedded finite fields

Edouard Rousseau

GT BAC  
December 14, 2017

# CONTENTS

## The embedding problem

- The problem

- Description

## The compatibility problem

- The problem

- Bosma, Cannon and Steel framework

- Computing an isomorphism with a common subfield

# 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  $\alpha_1, \alpha_2$  such that
  - ▶  $E = \mathbb{F}_p(\alpha_1)$
  - ▶ *there exists* an embedding  $\phi : E \rightarrow F$  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:

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

## Algorithm:

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

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  $\zeta$
- ▶ Solve  $\sigma(x) = \zeta x$  in  $E$ , where  $\sigma :=$  Frobenius automorphism (Hilbert 90)
  - ▶ Denote by  $\alpha_1$  a solution
- ▶ Solve  $\sigma(y) = \zeta y$  in  $F$ 
  - ▶ Denote by  $\alpha_2$  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  $\zeta$  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  $\alpha_1, \alpha_2$

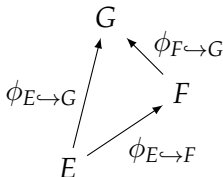


# The compatibility problem

# THE COMPATIBILITY PROBLEM

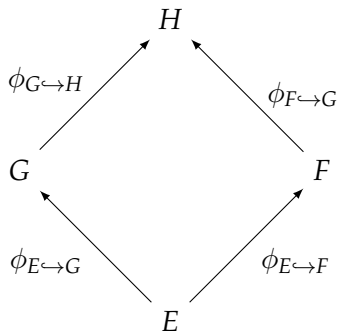
## Context:

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



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

## THE COMPATIBILITY PROBLEM II



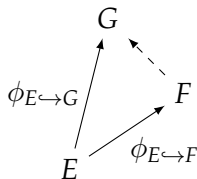
$$\phi_{G \hookrightarrow H} \circ \phi_{E \hookrightarrow G} \stackrel{?}{=} \phi_{F \hookrightarrow H} \circ \phi_{E \hookrightarrow F}$$

# 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



- ▶ Take  $\phi'_{F \hookrightarrow G}$  an arbitrary embedding between  $F$  and  $G$
- ▶ Find  $\sigma \in \text{Gal}(G/\mathbb{F}_p)$  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  $|\text{Gal}(F/E)|$  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  $\phi_{E \hookrightarrow F}$

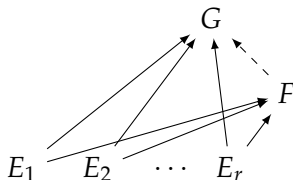
**CE2** (Reflexivity) For each  $E$ ,  $\phi_{E \hookrightarrow E} = \text{Id}_E$

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

**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)

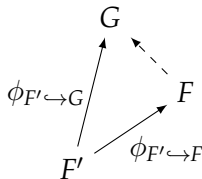
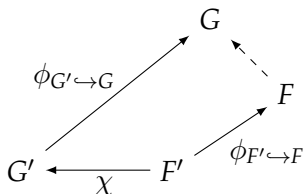


- ▶ Set  $F'$  the field generated by the fields  $E_i$  in  $F$
- ▶ Set  $G'$  the field generated by the fields  $E_i$  in  $G$

## Theorem

*There exists a unique isomorphism  $\chi : F' \rightarrow G'$  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)

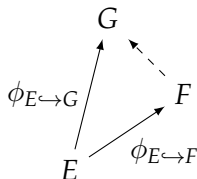


- ▶ We have  $|\text{Gal}(F/F')|$  compatible morphisms



# BOSMA, CANNON AND STEEL FRAMEWORK (PRACTICE)

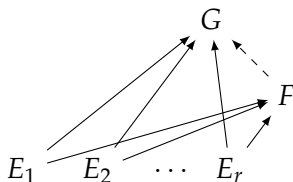
- ▶ Use the naive embedding algorithm



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

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

# BOSMA, CANNON AND STEEL FRAMEWORK (PRACTICE)



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

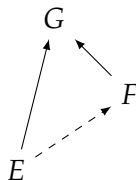
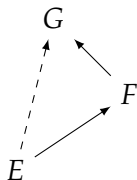
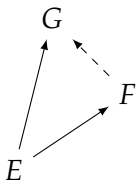
## BOSMA, CANNON AND STEEL FRAMEWORK

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

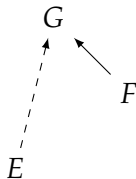
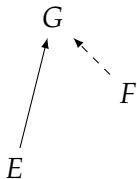
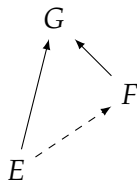
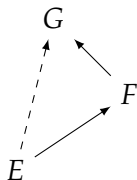
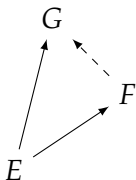
# BOSMA, CANNON AND STEEL FRAMEWORK

Some configurations with triangles:



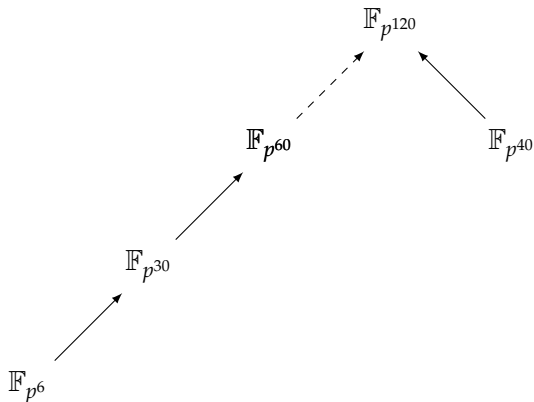
# BOSMA, CANNON AND STEEL FRAMEWORK

Some configurations with triangles:



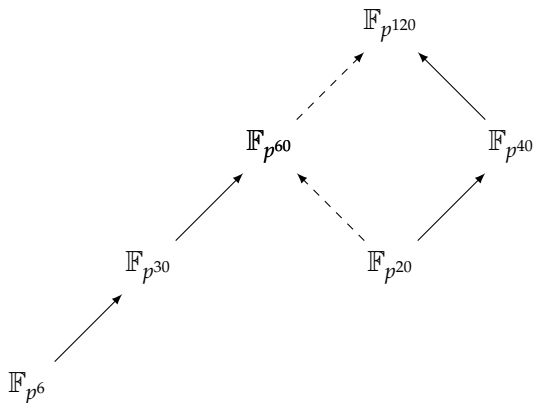
# BOSMA, CANNON AND STEEL FRAMEWORK

An example of what can happen with the intersections:



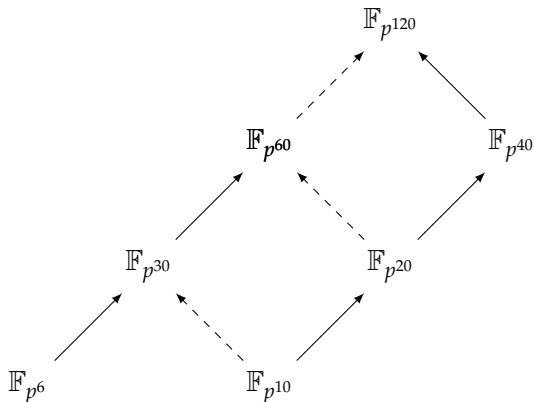
# BOSMA, CANNON AND STEEL FRAMEWORK

An example of what can happen with the intersections:



# BOSMA, CANNON AND STEEL FRAMEWORK

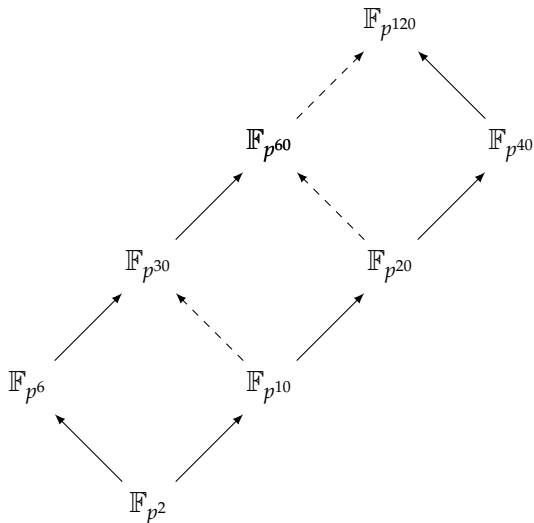
An example of what can happen with the intersections:





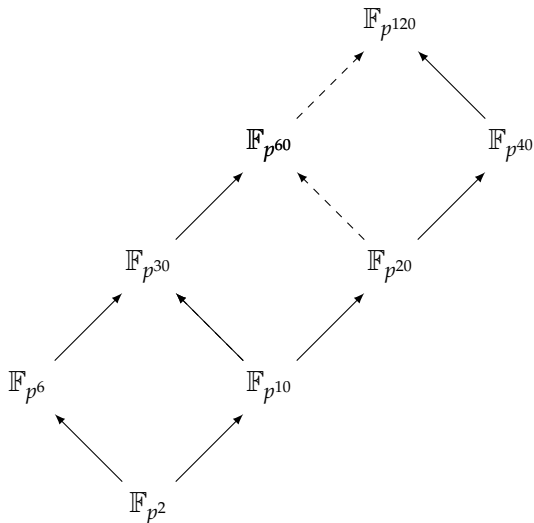
# BOSMA, CANNON AND STEEL FRAMEWORK

An example of what can happen with the intersections:



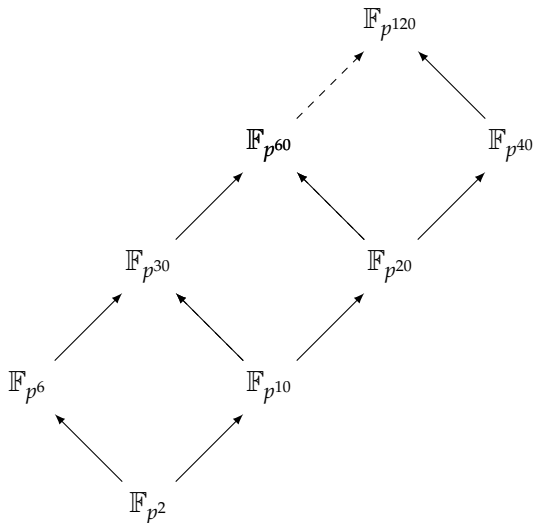
# BOSMA, CANNON AND STEEL FRAMEWORK

An example of what can happen with the intersections:



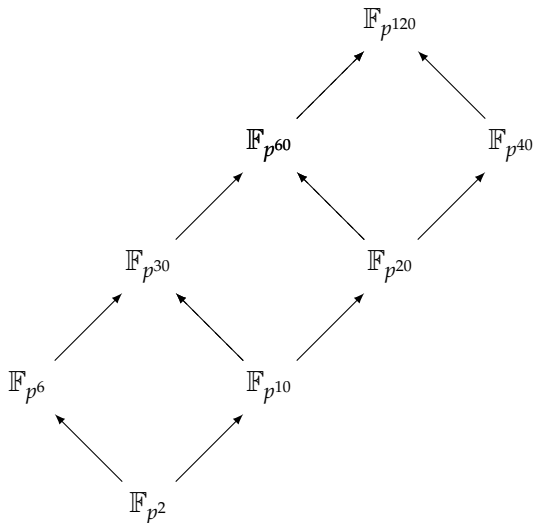
# BOSMA, CANNON AND STEEL FRAMEWORK

An example of what can happen with the intersections:



# BOSMA, CANNON AND STEEL FRAMEWORK

An example of what can happen with the intersections:



# COMPUTING AN ISOMORPHISM WITH A COMMON SUBFIELD

- ▶ We want to embed  $E$  in  $F$ 
  - ▶ additional 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  $S_1, S_2, \dots, S_r$  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 !