# Standard lattices of compatibly embedded finite fields

Luca De Feo Hugues Randriambololona

Édouard Rousseau

Lattices of compatibly embedded finite fields are useful in computer algebra systems for managing many extensions of a finite field $\mathbb{F}_p$ at once.

They can also be used to represent the algebraic closure $\bar{\mathbb{F}}_p$, and to represent all finite fields in a standard manner.

The most well known constructions are Conway polynomials [1, 2], and the Bosma–Cannon–Steel framework [3] used in Magma. They all have drawbacks : Conway polynomials are extremely expensive to compute, while the Bosma–Cannon–Steel framework does not provide a standard way to represent finite fields, and becomes inefficient as the number of extensions grows.

In this work, leveraging the theory of the Lenstra-Allombert isomorphism algorithm [4], we generalize at the same time Conway polynomials and the Bosma–Cannon–Steel framework : our construction can be used both to define new standard families of compatible polynomials defining finite fields, and to compute compatible embeddings between arbitrary finite fields. Our construction computes and evaluates chains of embeddings in quasi-quadratic time in the (largest) extension degree, and linear time in the number of extensions involved. Furthermore, our implementation written in C/Flint/Julia/Nemo shows that our construction is practical.

## Références

[1] Nickel, Werner. *Endliche Körper in dem gruppentheoretischen Programmsystem GAP.* https://www2.mathematik.tu-darmstadt.de/~nickel/

[2] Heath, Lenwood S. and Loehr, Nicholas A. *New algorithms for generating Conway polynomials over finite fields.* Proceedings of the tenth annual ACM-SIAM symposium on Discrete algorithms, **pages 429-437**.

[3] Bosma, Wieb and Cannon, John and Steel, Allan. *Lattices of compatibly embedded finite fields.* Journal of Symbolic Computation, **pages 351-369**.

[4] Bill Allombert. *Explicit Computation of Isomorphisms between Finite Fields.* Finite Fields Appl. **pages 332-342**.