Compatible lattices of finite fields

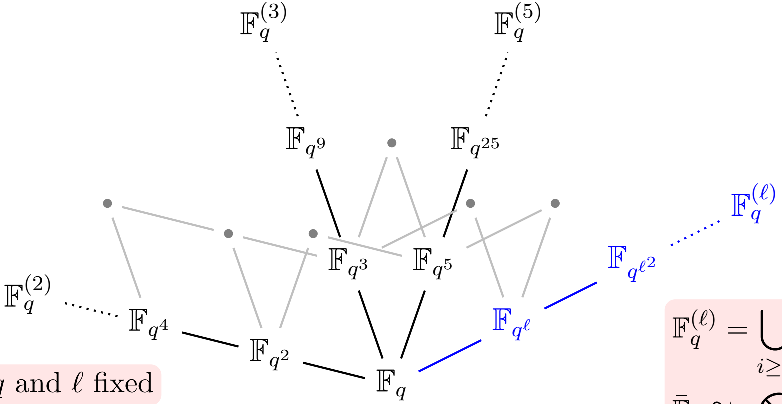
Luca De Feo[1]
joint work with Javad Doliskani[2], Éric Schost[2]

[1]Laboratoire PRiSM, Université de Versailles
[2]Department of Computer Science, Western University

Sage Days 52, September 4, 2013

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

Problem statement



q and ℓ fixed

$$\mathbb{F}_q^{(\ell)} = \bigcup_{i\geq 0} \mathbb{F}_{q^{\ell^i}},$$

$$\bar{\mathbb{F}}_q \cong \bigotimes_{\ell \text{ prime}} \mathbb{F}_q^{(\ell)}$$

What's a compatible lattice?

- A collection of finite fields $\mathbb{F}_{p^n}$ for $n > 1$;
- A collection of morphisms $\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$ whenever $m|n$.

Any element of $\bar{\mathbb{F}}_p$ (or $\bar{\mathbb{F}}_{p^n}$) can be represented as an element of the lattice.

How to build a compatible lattice?

Construct fields arbitrarily + compute isomorphisms

- Factor minimal polynomials (#13214),
- Rains' isomorphism algorithm (Magma),
- Allombert's isomorphism algorithm (Pari?),
- Linear algebra (Magma),
- Map generators (#13214).

Construct fields defined by *special* polynomials

- (pseudo)-Conway polynomials (Magma, Sage 5.13?),
- Cyclotomy theory (De Smit, Lenstra),
- Fancy (and still limited) constructions (Cantor, Couveignes, DF, Doliskani, Lercier, Schost).