The embedding problem

Let $\mathbb{F}_q$ be a field with $q$ elements, $m$ and $n$ be irreducible polynomials in $\mathbb{F}_q[X]$ and $\mathbb{F}_q[Y]$, respectively.

There exists a field embedding $\varphi: \mathbb{F}_q[X] \hookrightarrow \mathbb{F}_q$. We are interested in the unique up to $\mathbb{F}_q$-isomorphism of $k = \mathbb{F}_q[X]/(f)$.

Goals

- Represent $\varphi$ efficiently.
- Evaluate/Invert $\varphi$ efficiently.

When $deg f = deg g$, this also is called the isomorphism problem.

Applications

- Fundamental building blocks of algebraic system algorithms.
- Work algorithmically in the algebraic closure $\bar{\mathbb{F}}_q$.

Embedding description

Determine elements $\alpha \in k$ and $\beta \in K$ such that

- $\alpha$ generates $k = \mathbb{F}_q[\alpha]$,
- $\beta$ is a root of $f(X)$.
- $\beta \!\not\!|$ a root of $g(X)$.

Cost of factorization: $O(mn)$.

Kummer-type algorithms: Use properties of $m$-th roots of unity.

Group-based algorithms: Use properties of an algebraic group $G/\mathbb{F}_q$.

Embedding evaluation

Given

- A description of the embedding (as above).
- $\gamma \in k, \beta \in K$.

Solve the following problem:

- Compute $\varphi(\gamma) \in K$.
- Test if $\beta \!\not\!| \varphi(\gamma)$.
- Supposing $\in \varphi(\gamma)$, compute $\varphi^{-1}(\delta)$ in $k$.

Naive solution: Linear algebra (size $n \times m$).

KÜMMER-TYPE ALGORITHMS

Lenstra’s algorithm [7]

Goals

- Prove that the isomorphism problem is deterministic: polynomial, pervasive use of linear algebra.
- Does not prove precise complexity: $\Omega(mn)$.

Technique

- Reduce to a prime power.
- If $(n,q) > 1$.
  - use Artin-Schreier theory.
  - else use Kummer theory.
  - find $\alpha \in k \setminus \mathbb{F}_q$.
  - find $\beta \in K \setminus \mathbb{F}_q$.
  - compute $\varphi^{-1}(\delta)$.

In general, if $m | (q - 1)$, adjoint roots of unity by working in cyclotomic extensions.

Rain’s cyclotomic algorithm [10]

Removes trial-and-error

- Replace $\alpha, \beta$ with Gaussian periods.
  - $\varphi(\alpha)$ = a $m$-th root of $a$, with small $a$, take degree $\alpha$ extensions.
  - best bound: $= O(m^{2+\varepsilon}(GHR))$, in practice $= O(m\log m)$.

Practical complexity: $\tilde{O}(m^{2+\varepsilon})$. Fast when $\alpha = 1$.

Limitations

- Unpublished. Implemented in Magma.
- Only practical for very small $a$.

Elliptic curve variant

- Replace Gaussian periods with elliptic periods $[\ell]$, an Abelian prime.
- Same bounds on $\alpha = O(m^{2+\varepsilon}(GHR))$, $O(m\log m)$ (practical).
- Practical complexity: $\tilde{O}(m \log q)$.
- Sloppy and cyclic method for $\alpha = 1$.
- Works well with $q$ non-prime.

Embedding evaluation

Evaluation decomposition

A dual of polynomial evaluation $\mathbb{F}_q[Y]/(g) = K = \mathbb{F}_q[X]/(f)$.

$\beta$ Trivial.

$\gamma$ Evaluate polynomial in $\beta$ mod $g$.

$\varphi^{-1}$ Dual of $A \times B = C$.

Algorithms

- Polynomial evaluation
  - Horner’s rule: $\tilde{O}(mn)$.
  - Modular composition: $O(m^{1+\varepsilon})$ [8].

- Dual operations: same complexity as original (transposition principle).

Normal bases: All the previous algorithms yield a normal element $\alpha$. Conversions to/from normal bases $(A,C)$ can be done in $O((n^2+1)\log q)$ [5].

GROUP-BASED ALGORITHMS

Pinch’s algorithm [9]

Idea

- Find small $s$ s.t. $k \cong \mathbb{F}_q[\mu_s]$.
- Pick a set of roots of unity $\alpha, \beta \in k$.
- Find $e$ s.t. $\alpha^e = \beta$.

No complexity analysis, fast if $s$ small.

Technical details

- $s$ is the smallest integer s.t. $\deg_q(g) = m$.
- Problem: generally $s \not\in O(m)$. (\textit{Proof} [9]).
- Test if $\alpha^e \!\not\!| \beta$ by linear algebra.
- Problem: tests are expensive, possibly $O(s)$ of them.

Elliptic variant

- Replace $\mu_s$ by an $s$-torsion subgroup of an elliptic curve.
- Possibly more efficient for $s$; hopefully $s \in O(m)$.

Implementation

- $C/\text{Flint}$ implementation of Allombert’s algorithm. 
- Sage/Cython implementation of Rains’ and variants.
- Comparisons with Pari/GP, Sage, Magma, . . .

comparison of main algorithms

vants’ algorithms of Rains [2].

References