Polynomial factorization over finite fields

MPRI – Efficient algorithms in computer algebra

Pierre Lairez

Factorization reveals interesting phenomena

1. pick a random $f \in \mathbb{Q}[t, x, y]$
2. compute $\Delta = \mathrm{disc}_x(\mathrm{disc}_y(f))$
3. compute the irreducible factors of Δ

How to compute the irreducible factors of Δ?

1st step: factorization over $\mathbb{F}_q$, q odd ← today
2nd step: factorization over $\mathbb{Q}$

L. Busé, B. Mourrain (2009). “Explicit Factors of Some Iterated Resultants and Discriminants”. In: *Math. Comp.* 78.265, pp. 345–386. DOI: 10/ccjgkw

Much easier than factorization over $\mathbb{Z}$!

$\mathbb{F}_p[x]$ has many similarities with $\mathbb{Z}$:

- Euclidean division
- the degree in $\mathbb{F}_p[x]$ matches the logarithm of the absolute value in $\mathbb{Z}$
- similar data representation
- similar (fast) multiplication algorithms
- (sometimes) similar algorithms for matrices over $\mathbb{F}_p[x]$ or $\mathbb{Z}$

Factorization is where analogy breaks down!

General factorization is undecidable

Theorem (Van der Waerden 1930)

There exists an effective field K such that irreducibility in $K[x]$ is undecidable.

Proof

Take $K = \mathbb{Q}[\sqrt{p_{i_1}}, \sqrt{p_{i_2}}, \dots]$, where p_i is the ith prime number and $i_1, i_2, \dots$ is an enumeration of the indices of the Turing machines that halt. For a given i, does $X^2 - p_i$ splits over K? $\square$

The example itself is irrelevant. Interesting conclusion:

⚠ No factorization algorithm for abstract fields.
We will deal with specific properties of finite fields.

B. L. van der Waerden (1930). “Eine Bemerkung über die Unzerlegbarkeit von Polynomen”. In: *Math. Ann.* 102.1, pp. 738–739. DOI: 10/dmdkm6

Finite fields I

Lemma

If K is a finite field, then $|K|$ is a power of a prime number.

Proof

K is a $\mathbb{F}_p$-linear space, with $p = \operatorname{char} K$, so $|K| = |\mathbb{F}_p|^{\dim K}$. $\square$

We fix a prime number p and an algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$.

Lemma

For any $q = p^n$, the set $\{x \in \overline{\mathbb{F}_p} \mid x^q = x\}$ is a subfield of $\overline{\mathbb{F}_p}$.

Proof

It is closed under multiplication, inverse and addition because $x \mapsto x^q$ is a field endomorphism.

Finite field II

Definition

For any prime power $q = p^n$, $\mathbb{F}_q \doteq \{x \in \overline{\mathbb{F}_p} \mid x^q = x\}$

Theorem

For any finite field K, $K \simeq \mathbb{F}_{|K|}$.

Proof

Let $q = p^n = |K|$. Since K is a finite set, it is an algebraic extension of its prime field $\mathbb{F}_p$.
So there is an embedding $\phi : K \hookrightarrow \overline{\mathbb{F}_p}$. Note that $K \simeq \phi(K)$.
By Lagrange's theorem applied to the multiplicative group $K^\times$, we have $x^q = x$ for any $x \in K$. So $\phi(K) \subseteq \mathbb{F}_q$. By equality of cardinality, $\phi(K) = \mathbb{F}_q$. □

Irreducible polynomials I

Let K be a field.
A polynomial $f \in K[x]$ is *irreducible* (over K) if is not the product of two nonconstant polynomials.

Lemma

A polynomial $f \in K[x]$ is irreducible if and only if the quotient ring $K[x]/(f)$ is a field.

Theorem

For any $f \in K[x]$, there are distinct monic irreducible polynomials $g_1, \ldots, g_r$ and positive integers $e_1, \ldots, e_r$ such that $f = \mathrm{lc}(f) g_1^{e_1} \cdots g_r^{e_r}$.
They are uniquely determined up to permutation.

The usual proof is very non constructive!

Squarefree polynomials I

A polynomial $f \in K[x]$ is *squarefree* if f is not divided by h^2 for any nonconstant $h \in K[x]$.

Lemma

Let $f \in K[x]$. The following are equivalent:

1. *f is squarefree;*
2. *the exponents in the irreducible factorization of f are 1;*
3. *the quotient ring $K[x]/(f)$ is isomorphic to a product of fields;*
4. *zero is the only nilpotent element of $K[x]/(f)$.*

For a polynomial f which factors as $c\prod_i g_i^{e_i}$, the *squarefree part* of f is $\prod_i g_i$.

⚠ $\gcd(f, f') = 1 \Rightarrow f$ is squarefree. The converse is not true.

Squarefree polynomials II

Proof

Let $f = c\prod_i g_i^{e_i}$ be the irreducible factorization of f.

$1 \Rightarrow 2$. If $e_i > 1$ then g_i^2 divides f, so f is not squarefree.

$2 \Rightarrow 3$. If $f = c\prod_i g_i$ then $K[x]/(f) = \prod_i K[x]/(g_i)$. Since g_i is irreducible, $K[x]/(g_i)$ is a field.

$3 \Rightarrow 4$. Let $(\alpha_1, \ldots, \alpha_r)$ be a nilpotent element of a product $K_1 \times \cdots \times K_r$ of fields. That is $(\alpha_1^n, \ldots, \alpha_r^n) = (0, \ldots, 0)$ for some $n \geq 1$. Since each K_i is a field, this implies $\alpha_i = 0$.

$4 \Rightarrow 1$. Assume, for contradiction, that there is some nonconstant polynomial h such that $h^2|f$. Write $f = ah^2$. Then ah is nilpotent in $K[x]/(f)$. By hypothesis, ah is zero in this ring. So ah is divisible by f. But $\deg(ah) < \deg(f)$. $\square$

Finite fields are perfect

Let $q = p^n$ be a prime power.

Lemma

On $\mathbb{F}_q$, the field endomorphism $\mathrm{Frob} : \alpha \mapsto \alpha^p$ is bijective with inverse $\mathrm{Frob}^{n-1} : \alpha \mapsto \alpha^{p^{n-1}}$.

Proof

Frob is injective, as any field endomorphism, and so bijective because $\mathbb{F}_q$ is finite.
$\mathrm{Frob}^n(\alpha) = \alpha^q = \alpha$ (Lagrange's theorem), so $\mathrm{Frob}^{-1} = \mathrm{Frob}^{n-1}$. □

Lemma

For any $f \in \mathbb{F}_q[x]$, if $f' = 0$, then $f = g^p$ for some $g \in \mathbb{F}_q[x]$.

Proof

Let $f = \sum_i a_i x^i$. If $f' = 0$, then $a_i = 0$ unless $p | i$.
So $f = \sum_i a_{pi} x^{pi} = (\sum_i \mathrm{Frob}^{-1}(a_{pi}) x_i)^p$.

Reduction to squarefree

```
def SquarefreePart(f):
    if f and f' coprime:
        return f
    elif f' = 0:
        compute g such that f = g^p
        return SquarefreePart(g)
    else:
        h ← f/gcd(f, f')
        g ← f/gcd(f, h^(deg f))    [g' = 0]
        return h · SquarefreePart(g)
```

Theorem

On input $f \in \mathbb{F}_q[x]$ nonzero of degree d, SquarefreePart outputs the squarefree part of f and performs $O(M(d)\log d + dp^{-1}\log q)$ operations in $\mathbb{F}_q$.

Recap

$f \in \mathbb{F}_q[x]$

$M(d) \log d + \frac{d}{p} \log q$

squarefree part of f

⚠ to do

irreducible factors of f

$dM(d)$ with the naive algorithm

irreducible decomposition of f

Berlekamp's irreducibility test

Let $f \in \mathbb{F}_q[x]$ squarefree.
The map $Q : \alpha \mapsto \alpha^q$ is a $\mathbb{F}_q$-linear map on $\mathbb{F}_q[x]/(f)$.

Theorem (Berlekamp 1967)

$\dim_{\mathbb{F}_q} \ker(Q - \mathrm{id})$ *equals the number of irreducible factors of* f.

Proof

Decompose $\mathbb{F}_q[x]/(f)$ as $L_1 \times \cdots \times L_r$, where each L_i is an algebraic extension of $\mathbb{F}_q$.
Each factor L_i is stable under Q. In particular

$$\begin{aligned} \ker(Q - \mathrm{id}) &\simeq \textstyle\prod_i \ker(Q - \mathrm{id})|_{L_i} \\ &= \textstyle\prod_i \{\alpha \in L_i \mid \alpha^q = \alpha\} = \mathbb{F}_q^r. \qquad \square \end{aligned}$$

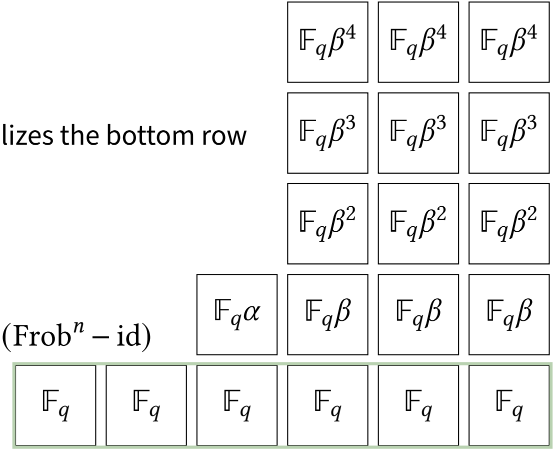
Corollary

Irreducibility in $\mathbb{F}_q[x]$ is decidable with $O(d^\omega + dM(d)\log q)$ operations in $\mathbb{F}_q$, where d is the degree.

The quotient ring of a squarefree polynomial

Frob^n stabilizes the bottom row

$\ker(\mathrm{Frob}^n - \mathrm{id})$



$$\mathbb{F}_q[x]/(f) \simeq \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_{q^2} \times \mathbb{F}_{q^5} \times \mathbb{F}_{q^5} \times \mathbb{F}_{q^5}$$

Factorization: a trivial but key idea

Lemma

Let $f \in K[x]$ be a squarefree polynomial.
Let $f = g_1 \cdots g_r$ be its irreducible decomposition.

Let $\eta \in K[x]/(f)$ and $(\eta_1, \ldots, \eta_r)$ the corresponding tuple under the isomorphism $K[x]/(f) \simeq K[x]/(g_1) \times \cdots \times K[x]/(g_r)$.

Then $\gcd(f, \eta) = \prod_{i \text{ s.t. } \eta_i = 0} g_i$.

Proof

$\eta_i = 0 \Leftrightarrow g_i | \eta$. □

We want to find an η with some but not all zero components.

Squares in $\mathbb{F}_q$

⚠ Assumption: q is odd

Lemma

Let $S_+ = \left\{\alpha \in \mathbb{F}_q^\times \,\middle|\, \alpha^{\frac{q-1}{2}} = 1\right\}$ *and* $S_- = \left\{\alpha \in \mathbb{F}_q^\times \,\middle|\, \alpha^{\frac{q-1}{2}} = -1\right\}$.

Then

1. $\#S_+ = \#S_- = \frac{q-1}{2}$
2. $\mathbb{F}_q^\times$ *is the disjoint union of* S_+ *and* S_-.

Proof

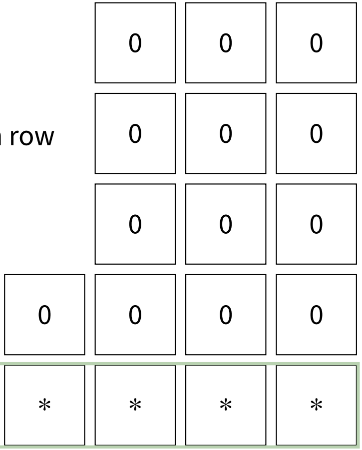
As the zero set of polynomials of degree $\frac{q-1}{2}$, S_+ and S_- contain at most $\frac{q-1}{2}$ elements each.

For any $\alpha \in \mathbb{F}_q^\times$, $1 = \alpha^{q-1} = (\alpha^{\frac{q-1}{2}})^2$, so $\mathbb{F}_q^\times = S_+ \cup S_-$. The union is clearly disjoint. For cardinality reasons, $\#S_+ = \#S_- = \frac{q-1}{2}$.

Berlekamp's idea for factorization

Frob^n stabilizes the bottom row

$\ker(\mathrm{Frob}^n - \mathrm{id})$



$$\mathbb{F}_q[x]/(f) \simeq \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_{q^2} \times \mathbb{F}_{q^5} \times \mathbb{F}_{q^5} \times \mathbb{F}_{q^5}$$

1. Compute $\ker(\mathrm{Frob}^n - \mathrm{id})$
2. Choose a uniformly distributed random element in it
3. Elevate to the power $\frac{q-1}{2}$
4. Add 1
5. Takes the gcd with f

⚠ Assumption: q is odd

Distinct-degree factorization

$\eta \leftarrow$ class of x

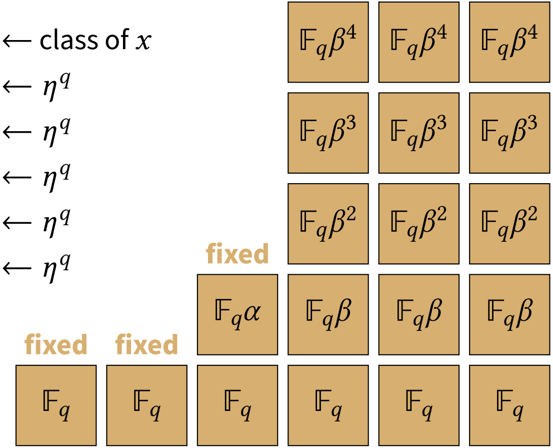
$\eta \leftarrow \eta^q$

$\eta \leftarrow \eta^q$

$\eta \leftarrow \eta^q$

$\eta \leftarrow \eta^q$

$\eta \leftarrow \eta^q$



$$\mathbb{F}_q[x]/(f) \simeq \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_{q^2} \times \mathbb{F}_{q^5} \times \mathbb{F}_{q^5} \times \mathbb{F}_{q^5}$$

A formula for irreducible polynomials I

As usual, let $q = p^n$ be a prime power.

Lemma

Let $\mathcal{P}_d = \left\{ g \in \mathbb{F}_q[x] \,\middle|\, g \text{ is monic, irreducible and of degree } d \right\}$.
For any $d \geq 1$,

$$x^{q^d} - x = \prod_{s \mid d} \prod_{g \in \mathcal{P}_s} g.$$

A complete description of the irreducible polynomials over $\mathbb{F}_q$!

Proof

A formula for irreducible polynomials II

Let $g \in \mathcal{P}_s$ for some divisor s of d. The quotient ring $\mathbb{F}_q[x]/(g)$ is a field of cardinality q^s.
In particular, its generator $\alpha \doteq [x]$ satisfies $\alpha = \alpha^{q^s} = \alpha^{q^d}$. So g divides $x^{q^d} - x$.
It follows that $\prod_{s|d} \prod_{g \in \mathcal{P}_s} g$ divides $x^{q^d} - x$.

Conversely, let g be an irreducible factor of $x^{q^d} - x$. The quotient ring $\mathbb{F}_q[x]/(g)$ is a field and its generator $\alpha = [x]$ satisfy $\alpha^{q^d} = \alpha$. So it is a subfield of $\mathbb{F}_{q^d}$ and therefore isomorphic to some $\mathbb{F}_{q^s}$, for some divisor s of d. It follows that the minimal polynomial of α (that is g) has degree s.
To conclude, observe that the l.h.s. is squarefree (its derivative is -1).

Distinct-degree factorization, the algorithm

input $f \in \mathbb{F}_q[x]$ monic and squarefree

output $g_1, \ldots, g_s \in \mathbb{F}_q[x]$ such that $f = g_1 \cdots g_s$ and the irreducible factors of g_i have degree i.

```
def DistinctDegreeFactor(f):
    s ← 0
    η ← x
    while f is not constant:
        s ← s + 1
        η ← η^q  mod f    [η = x^(q^s)  mod f]
        g_s ← gcd(η − x, f)
        f ← f / g_s
    return (g_1, ..., g_s)
```

Theorem

The algorithm is correct and performs $O(dM(d)\log d + dM(d)\log q)$ operations in $\mathbb{F}_q$.

Cantor and Zassenhaus' idea

Assumption: q is odd

$= 0$	$\neq 0$ $\in S_+$	$\neq 0$ $\in S_+$	$\neq 0$ $\in S_-$	$\neq 0$ $\in S_+$
$*$	$*$	$*$	$*$	$*$
$*$	$*$	$*$	$*$	$*$
$*$	$*$	$*$	$*$	$*$

$$\mathbb{F}_q[x]/(f) \simeq \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3}$$

1. pick η at random
2. $\eta \leftarrow \eta^{\frac{q^3-1}{2}}$
3. $f = \gcd(f, \eta)\gcd(f, \eta - 1)\gcd(f, \eta + 1)$

Cantor and Zassenhaus' theorem I

⚠ Assumption: q is odd

Theorem (Cantor, Zassenhaus 1981)

Let $f \in \mathbb{F}_q[x]$ of degree d such that all irreducible factors of f have degree $s < d$. (Note that $s|d$.)
Let $\eta \in \mathbb{F}_q[x]$ be a polynomial of degree less than d.
Then

1. $f = \gcd(f, \eta) \cdot \gcd(f, \eta^{\frac{q^s-1}{2}} - 1) \cdot \gcd(f, \eta^{\frac{q^s-1}{2}} + 1)$
2. *for at least 50% of the q^d possible choices of η, the factorization above is nontrivial.*

D. G. Cantor, H. Zassenhaus (1981). "A New Algorithm for Factoring Polynomials over Finite Fields". In: *Math. Comput.* 36.154, pp. 587–592. DOI: 10/b652qb

Cantor and Zassenhaus' theorem II

Proof

We just proved the first point.

Concerning the second point, let $\eta \in \mathbb{F}_q[x]/(f)$ and $(\eta_1, \ldots, \eta_r)$ its decomposition in $\prod_i \mathbb{F}_q[x]/(g_i) = (\mathbb{F}_{q^s})^r$, where $f = g_1 \cdots g_r$. We have a trivial factorization if and only if the η_i are all zero, or all in S_+ or all in S_-. Therefore

$$\begin{aligned} \mathrm{Prob}(\text{trivial factorization}) &= \frac{1 + \#S_+^r + \#S_-^r}{\text{total number of choices}} \\ &= q^{-d}\left(1 + 2\left(\frac{q^s - 1}{2}\right)^r\right) \\ &\leq q^{-d}\left(2^{1-r}(q^s)^r\right) = 2^{1-r} \leq \frac{1}{2}. \qquad \square \end{aligned}$$

Cantor and Zassenhaus' algorithm

input $f \in \mathbb{F}_q[x]$ squarefree, $s < \deg f$ such that the irreducible factors of f have degree s

output the irreducible factors of f

def *CZ*(f, s)**:**
    if $s = \deg f$**:**
        return $\{f\}$
    else:
        pick $a_0, \ldots, a_{\deg f - 1} \in \mathbb{F}_q$ uniformly at random
        $\eta \leftarrow a_0 + a_1 x + \cdots + a_{\deg f - 1} x^{\deg f - 1}$
        $\eta \leftarrow \eta^{\frac{q^s - 1}{2}} \mod f$
        $g_0 \leftarrow \gcd(f, \eta)$
        $g_+ \leftarrow \gcd(f, \eta - 1)$
        $g_- \leftarrow \gcd(f, \eta + 1)$ $[g_- = f / g_0 / g_+]$
        return *CZ*$(g_0, s) \cup$ *CZ*$(g_+, s) \cup$ *CZ*(g_-, s)

Application/exercise

Let $p = 2^{61} - 1$.
Compute $u \in \mathbb{F}_p$ such that $u^2 = 5$.

Complexity analysis

Excluding recursive calls, each call performs:

- $O(M(d) \log d)$ ops in $\mathbb{F}_q$ for the gcd computations
- $O(M(d) s \log q)$ ops in $\mathbb{F}_q$ for the exponentiation

A recursive call is *trivial* if the degree of its argument has not decreased. On average, there is no more than 50% trivial calls. There are $O(d)$ nontrivial calls. So there are $O(d)$ calls on average.
This leads to a $O(sdM(d) \log q + dM(d) \log d)$ total average complexity.

⚠ This is not a tight analysis!

Refined complexity analysis

Imagine a biased dice with 3 facets:

- a facet $\bigcirc$ with probability $q^{-s} \leq \frac{1}{3}$
- two equiprobable facets $\oplus$ and $\ominus$

Game

Draw r columns. At each turn, draw one dice for each column, and append the symbol to the column. Stop when each column is different.

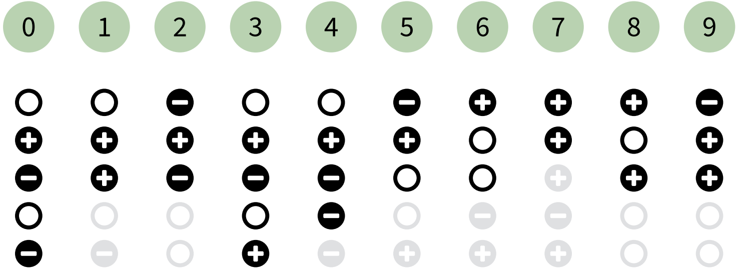
Lemma

The game stops after $O(\log r)$ iterations on average.

Proof

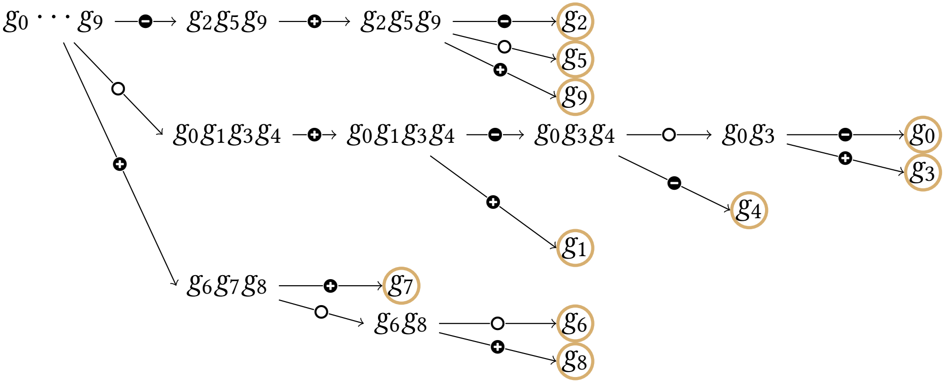
The probability that the columns i and j are equal after k iterations is at most 2^{-k}. The probability that the columns are not all different after k iterations is at most $r^2 2^{-k}$. $\square$

Let us play



(Probably more ○ than what would happen in practice.)

Another view of the game



This is the tree of recursive calls in CZ algorithm.

The tree has height $O(\log r)$ on average. The sum of the cost of all computations at a given depth is $O(M(d) s \log q + M(d) \log d)$.

Total average complexity: $O\left((M(d) s \log q + M(d) \log d) \log r\right)$.

The full algorithm...

```
def Factor(f):
    f_squarefree ← SquarefreePart(f)
    g_1, ..., g_s ← DistinctDegreeFactor(f_squarefree)
    𝓘 ← ∅
    for i ∈ {1, ..., s}:
        𝓘 ← 𝓘 ∪ CZ(g_i, i)
    𝓙 ← ∅
    for g ∈ 𝓘:
        e ← 0
        while true:
            f ← f/g
            e ← e + 1
            if g does not divides f:
                break
        𝓙 ← 𝓙 ∪ {(g, e)}
    return 𝓙
```

...and its complexity

Theorem (Cantor, Zassenhaus 1981)

The algorithm above, on input $f \in \mathbb{F}_q[x]$, outputs the irreducible factorization of f after

$$O(dM(d)(\log d + \log q)) = \tilde{O}(d^2 \log q)$$

operations in $\mathbb{F}_q$, where $d = \deg f$.

Major open question

Can we factor polynomials over $\mathbb{F}_q$ in deterministic polynomial time?

J. von zur Gathen, V. Shoup (1992). “Computing Frobenius Maps and Factoring Polynomials”. In: *Comput Complexity* 2.3, pp. 187–224. DOI: 10/dmbbhb

E. Kaltofen, V. Shoup (1998). “Subquadratic-Time Factoring of Polynomials over Finite Fields”. In: *Math. Comp.* 67.223, pp. 1179–1197. DOI: 10/c3ttb3

K. S. Kedlaya, C. Umans (2011). “Fast Polynomial Factorization and Modular Composition”. In: *SIAM J. Comput.* 40.6, pp. 1767–1802. DOI: 10/fxv98c

The iterated Frobenius algorithm

input $f \in \mathbb{F}_q[x], \eta \in \mathbb{F}_q[x]$, and $\leq s \leq \deg f$, with $\deg \eta < \deg f$

output $\eta, \eta^q, \eta^{q^2}, \ldots, \eta^{q^s} \mod f$

def *IteratedFrobenius*(f, η, s)**:**

    $\gamma_0 \leftarrow x$

    $\gamma_1 \leftarrow x^q \mod f$

    while $i \leq s$**:**

        for $j \in \{1, \ldots, i\}$**:** [multipoint evaluation over the ring $\mathbb{F}_q[x]/(f)$]

            $\gamma_{i+j} \leftarrow \gamma_i(\gamma_j) \mod f$

        $i \leftarrow 2i$

    for $i \in \{0, \ldots, s\}$**:** [multipoint evaluation again]

        $\alpha_i \leftarrow \eta(\gamma_i) \mod f$

    return $\alpha_0, \ldots, \alpha_s$

What is going on?

1. For any $\eta \in \mathbb{F}_q[x]$, $\eta^{q^j} \equiv \eta(x^{q^j}) \equiv \eta(x^{q^j} \pmod f) \mod f$
2. Let $\gamma_i = x^{q^i} \mod f$.
   Using with $\eta = \gamma_i$, we have $\gamma_{i+j} \equiv (x^{q^i})^{q^j} \equiv \gamma_i(\gamma_j) \mod f$

Theorem

Algorithm IteratedFrobenius is correct and performs $O(M(d)^2 \log(d)^2 + M(d) \log q)$ operations in $\mathbb{F}_q$.

We can use this algorithm to improve the complexity of distinct-degree and equal-degree factorization.

The iterated Frobenius algorithm

input $f \in \mathbb{F}_q[x], \eta \in \mathbb{F}_q[x]$, and $s \geq 1$, with $\deg \eta < \deg f$

output $\eta^{\frac{q^s-1}{2}} \mod f$

def *SuperFastExponentiation*(f, η, s)**:**

$\alpha_0, \ldots, \alpha_{s-1} \leftarrow$ *IteratedFrobenius*$(f, \eta, s-1)$

return $(\alpha_0 \cdots \alpha_{s-1})^{\frac{q-1}{2}} \mod f$

NB: $\eta^{\frac{q^s-1}{2}} = \left(\prod_{i=0}^{s-1} \eta^{q^i}\right)^{\frac{q-1}{2}}$

Theorem

Algorithm SuperFastExponentiation is correct and performs $O(M(d)^2(\log d)^2 + M(d)\log q)$ operations in $\mathbb{F}_q$.

Final complexity result

Theorem (von zur Gathen, Shoup 1992)

The algorithm explained above, on input $f \in \mathbb{F}_q[x]$, outputs the irreducible factorization of f after

$$\tilde{O}(d^2 + d \log q)$$

operations in $\mathbb{F}_q$, where $d = \deg f$.