Factoring Polynomials of the form $f(x^n) \in \mathbb{F}_q[x]$

Fabio E. Brochero Martínez

joint work with Lucas da Silva Reis

CIMPA Research School
Algebraic Methods in Coding Theory

Universidade Federal de Minas Gerais
Instituto de Ciências Exatas
Departamento de Matemática

July 11, 2017

Motivations

Motivations

- A $[n,k]_q$-code $\mathcal{C}$ is called cyclic if it is invariant by the shift permutation, i.e.,

  if $(a_1, a_2, \ldots, a_n) \in \mathcal{C}$ then the shift $(a_n, a_1, \ldots, a_{n-1})$ is also in $\mathcal{C}$.

Motivations

- A $[n,k]_q$-code $\mathcal{C}$ is called cyclic if it is invariant by the shift permutation, i.e.,

  if $(a_1, a_2, \ldots, a_n) \in \mathcal{C}$ then the shift $(a_n, a_1, \ldots, a_{n-1})$ is also in $\mathcal{C}$.
- Since $\mathbb{F}_q^n$ is isomorphic to $\mathcal{R}_n = \frac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$, subspaces of $\mathcal{R}_n$ invariant by a shift are ideals and $\mathcal{R}_n$ is a principal ideal domain, it follows that each ideal is generated by a polynomial $g(x) \in \mathcal{R}_n$, where g is a divisor of $x^n - 1$.

Motivations

- A $[n,k]_q$-code $\mathcal{C}$ is called cyclic if it is invariant by the shift permutation, i.e.,

  if $(a_1, a_2, \dots, a_n) \in \mathcal{C}$ then the shift $(a_n, a_1, \dots, a_{n-1})$ is also in $\mathcal{C}$.
- Since $\mathbb{F}_q^n$ is isomorphic to $\mathcal{R}_n = \frac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle}$, subspaces of $\mathcal{R}_n$ invariant by a shift are ideals and $\mathcal{R}_n$ is a principal ideal domain, it follows that each ideal is generated by a polynomial $g(x) \in \mathcal{R}_n$, where g is a divisor of $x^n - 1$.
- Codes generated by a polynomial of the form $\frac{x^n-1}{h(x)}$, where h is an irreducible factor of $x^n - 1$, are called minimal cyclic codes.

The polynomial $x^n - 1 \in \mathbb{F}_q[x]$ splits into monic irreducible factors as $x^n - 1 = f_1 f_2 \cdots f_r$ by the Chinese Remainder Theorem

$$\mathcal{R}_n = \frac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle} \simeq \bigoplus_{j=1}^{r} \frac{\mathbb{F}_q[x]}{\langle f_j\rangle}$$

The polynomial $x^n - 1 \in \mathbb{F}_q[x]$ splits into monic irreducible factors as $x^n - 1 = f_1 f_2 \cdots f_r$ by the Chinese Remainder Theorem

$$\mathcal{R}_n = \frac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle} \simeq \bigoplus_{j=1}^{r} \frac{\mathbb{F}_q[x]}{\langle f_j\rangle}$$

so every primitive idempotent generates a maximal ideal of $\mathcal{R}_n$ and also one component of this direct sum.

The polynomial $x^n - 1 \in \mathbb{F}_q[x]$ splits into monic irreducible factors as $x^n - 1 = f_1 f_2 \cdots f_r$ by the Chinese Remainder Theorem

$$\mathcal{R}_n = \frac{\mathbb{F}_q[x]}{\langle x^n - 1\rangle} \simeq \bigoplus_{j=1}^{r} \frac{\mathbb{F}_q[x]}{\langle f_j\rangle}$$

so every primitive idempotent generates a maximal ideal of $\mathcal{R}_n$ and also one component of this direct sum.

Lemma

Let $\mathbb{F}_q$ be a finite field with q elements and n be a positive integer such that $\gcd(q, n) = 1$. Then every primitive idempotent of the group algebra $\mathcal{R}_n$ is of the form

$$e_f = -\frac{((f^*)')^*}{n} \cdot \frac{x^n - 1}{f},$$

where $f(x) \in \mathbb{F}_q[x]$ is an irreducible factor of $x^n - 1$.

Example

It is well known that

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

in any field, where $\Phi_d(x)$ denotes the d-th cyclotomic polynomial.

Example

It is well known that

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

in any field, where $\Phi_d(x)$ denotes the d-th cyclotomic polynomial.
In addition $\Phi_d(x)$ can be factor in $\frac{\varphi(d)}{ord_d q}$ irreducible factor of degree $ord_d q$.

Example

It is well known that

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

in any field, where $\Phi_d(x)$ denotes the d-th cyclotomic polynomial.
In addition $\Phi_d(x)$ can be factor in $\frac{\varphi(d)}{ord_d q}$ irreducible factor of degree $ord_d q$.
Then $\Phi_d(x)$ is an irredutible polynomial

Example

It is well known that

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

in any field, where $\Phi_d(x)$ denotes the d-th cyclotomic polynomial.
In addition $\Phi_d(x)$ can be factor in $\frac{\varphi(d)}{ord_d q}$ irreducible factor of degree $ord_d q$.
Then $\Phi_d(x)$ is an irredutible polynomial if and only if $ord_d q = \varphi(d)$

Example

It is well known that

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

in any field, where $\Phi_d(x)$ denotes the d-th cyclotomic polynomial.
In addition $\Phi_d(x)$ can be factor in $\frac{\varphi(d)}{ord_d q}$ irreducible factor of degree $ord_d q$. Then $\Phi_d(x)$ is an irredutible polynomial if and only if $ord_d q = \varphi(d)$ if and only if

1. $d = 2$ and q is odd
2. $d = 4$ and $q \equiv 3 \pmod 4$
3. $d = p^k$, p is a odd prime and $\langle g \rangle = \mathcal{U}(\mathbb{Z}_{p^k})$
4. $d = 2p^k$, p is a odd prime and $\langle g \rangle = \mathcal{U}(\mathbb{Z}_{2p^k})$

Question

Determine explicitly every irreducible factor of $x^n - 1 \in \mathbb{F}_q[x]$

Question

Determine explicitly every irreducible factor of $x^n - 1 \in \mathbb{F}_q[x]$

In general,

Question

Given $f(x) \in \mathbb{F}_q[x]$ *irreducible polynomial of degree* m *and order* e *and* n *a positive integer, determine explicitly every irreducible factor of* $f(x^n)$

Question

Determine explicitly every irreducible factor of $x^n - 1 \in \mathbb{F}_q[x]$

In general,

Question

Given $f(x) \in \mathbb{F}_q[x]$ *irreducible polynomial of degree* m *and order* e *and* n *a positive integer, determine explicitly every irreducible factor of* $f(x^n)$

Question

When $f(x^n)$ *is an irreducible polynomial and when* $f(x^n)$ *splits into* n *irreducible factors?*

Theorem (Lidl-Niederreiter Theorem 3.35)

Let n be a positive integer and $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m and order e. Then the polynomial $f(x^n)$ is irreducible over $\mathbb{F}_q$ if and only if the following conditions are satisfied:

Theorem (Lidl-Niederreiter Theorem 3.35)

Let n be a positive integer and $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m and order e. Then the polynomial $f(x^n)$ is irreducible over $\mathbb{F}_q$ if and only if the following conditions are satisfied:

1. *Every prime divisor of n divides e,*

Theorem (Lidl-Niederreiter Theorem 3.35)

Let n be a positive integer and $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m and order e. Then the polynomial $f(x^n)$ is irreducible over $\mathbb{F}_q$ if and only if the following conditions are satisfied:

1. *Every prime divisor of n divides e,*
2. $\gcd(n, (q^m - 1)/e) = 1$

Theorem (Lidl-Niederreiter Theorem 3.35)

Let n be a positive integer and $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m and order e. Then the polynomial $f(x^n)$ is irreducible over $\mathbb{F}_q$ if and only if the following conditions are satisfied:

1. *Every prime divisor of n divides e,*
2. $\gcd(n, (q^m - 1)/e) = 1$
3. *if $4|n$ then $4|q^m - 1$.*

In addition, in the case where the polynomial $f(x^n)$ is irreducible, it has degree mn and order en.

Theorem (Lidl-Niederreiter Theorem 3.35)

Let n be a positive integer and $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m and order e. Then the polynomial $f(x^n)$ is irreducible over $\mathbb{F}_q$ if and only if the following conditions are satisfied:

1. *Every prime divisor of n divides e,*
2. $\gcd(n, (q^m - 1)/e) = 1$
3. *if $4|n$ then $4|q^m - 1$.*

In addition, in the case where the polynomial $f(x^n)$ is irreducible, it has degree mn and order en.

Remark

Observe that the conditions (1) and (2) of Theorem before can be rewritten as

$$\nu_p(e) \geq 1 \quad \text{and} \quad \nu_p(q^m - 1) = \nu_p(e)$$

for every prime divisor p of n.

Theorem (Butler)

Let $f(x) \in \mathbb{F}_q[x]$ be a irreducible polynomial of degree m and order e. Let n be a positive integer such that $\gcd(n, q) = 1$.

1. *If $rad(n)$ divides e, then $f(x^n)$ splits in exactly $\frac{mn}{ord_{ne} q}$ irreducible factors of degree $ord_{ne} q$ and order ne.*

Theorem (Butler)

Let $f(x) \in \mathbb{F}_q[x]$ be a irreducible polynomial of degree m and order e. Let n be a positive integer such that $\gcd(n, q) = 1$.

1. *If $rad(n)$ divides e, then $f(x^n)$ splits in exactly $\frac{mn}{ord_{ne} q}$ irreducible factors of degree $ord_{ne} q$ and order ne.*
2. *If $gcd(n, e) = 1$, then for each d divisor of n, $f(x^n)$ has in its factorization exactly $m\frac{\phi(d)}{ord_{de} q}$ irreducible factors of degree $ord_{de} q$ and order de. In addition, every irreducible factor is of this type.*

Theorem (Butler)

Let $f(x) \in \mathbb{F}_q[x]$ be a irreducible polynomial of degree m and order e. Let n be a positive integer such that $\gcd(n, q) = 1$.

1. *If $rad(n)$ divides e, then $f(x^n)$ splits in exactly $\frac{mn}{ord_{ne} q}$ irreducible factors of degree $ord_{ne} q$ and order ne.*
2. *If $gcd(n, e) = 1$, then for each d divisor of n, $f(x^n)$ has in its factorization exactly $m\frac{\phi(d)}{ord_{de} q}$ irreducible factors of degree $ord_{de} q$ and order de. In addition, every irreducible factor is of this type.*

Remark

$f(x^n)$ splits into n irreducible factors if $ord_{ne} q = ord_e q$. Since $m = ord_e q$, the condition is equivalent to $\nu_p(q^m - 1) \geq \nu_p(n) + \nu_p(e)$ for all p prime divisor of n.

Lemma

Let $f(x)$ be an irreducible polynomial of degree m and exponent e. Let $n > 1$ be a positive divisor of $q-1$ such that

$$\nu_p(n) + \nu_p(e) \leq \nu_p(q-1) + \nu_p(ord_{r_p} q)$$

for all prime divisors p of n, where r_p is the largest divisor of e prime with p, i.e., $r_p = \frac{e}{p^{\nu_p(e)}}$. Then the polynomial $f(x^n)$ splits as a product of n irreducible polynomials of degree m. In addition, if $g(x)$ is any monic irreducible factor of $f(x^n)$ and c is any element of $\mathcal{U}(n)$, then

$$f(x^n) = \prod_{i=0}^{n-1} [c^{-mj} g(c^j x)]$$

is the factorization of $f(x^n)$ into irreducible factors.

Remark

Since

$$\nu_p(q^m - 1) \geq \nu_p(q-1) + \nu_p(ord_{r_p} q) \geq \nu_p(e) + \nu_p(n)$$

for all prime divisors p of n, and then the condition on Lemma is a sufficient (but not necessary) condition for $f(x^n)$ being a reducible polynomial.

Remark

Since

$$\nu_p(q^m - 1) \geq \nu_p(q-1) + \nu_p(ord_{r_p} q) \geq \nu_p(e) + \nu_p(n)$$

for all prime divisors p of n, and then the condition on Lemma is a sufficient (but not necessary) condition for $f(x^n)$ being a reducible polynomial.

Definition

Let $f(x) \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree m and exponent e. We say that the pair $\langle f(x), n \rangle$ satisfies the *reducible condition* if

$$\nu_p(q-1) \geq \nu_p(n) + \nu_p(e)$$

for every prime divisor p of n.

Theorem

Let $f(x) \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree m and exponent e, and let p^t be such that $\langle f(x), p^t \rangle$ satisfies the reducible condition. Suppose that $k = \nu_p(e)$ and $e = p^k r$. Then

(a) *There exists an unique element $c \in \mathbb{F}_q$ such that $f(x)$ divides $x^r - c$.*

Theorem

Let $f(x) \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree m and exponent e, and let p^t be such that $\langle f(x), p^t \rangle$ satisfies the reducible condition. Suppose that $k = \nu_p(e)$ and $e = p^k r$. Then

(a) *There exists an unique element $c \in \mathbb{F}_q$ such that $f(x)$ divides $x^r - c$.*

(b) *Let s be the solution of $sr \equiv 1 \pmod{p^t}$ with $0 < s < p^t$ and let $l = \frac{sr-1}{p^t}$. If $\alpha \in \overline{\mathbb{F}}_q$ is a root of $f(x)$, the polynomial $g(x) = \prod_{j=1}^{m}(x - b^s \alpha^{-lq^j})$ is an irreducible factor of $f(x^{p^t})$ over $\mathbb{F}_q$.*

Theorem

Let $f(x) \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree m and exponent e, and let p^t be such that $\langle f(x), p^t \rangle$ satisfies the reducible condition. Suppose that $k = \nu_p(e)$ and $e = p^k r$. Then

(a) *There exists an unique element $c \in \mathbb{F}_q$ such that $f(x)$ divides $x^r - c$.*

(b) *Let s be the solution of $sr \equiv 1 \pmod{p^t}$ with $0 < s < p^t$ and let $l = \frac{sr-1}{p^t}$. If $\alpha \in \overline{\mathbb{F}}_q$ is a root of $f(x)$, the polynomial $g(x) = \prod_{j=1}^{m}(x - b^s \alpha^{-lq^j})$ is an irreducible factor of $f(x^{p^t})$ over $\mathbb{F}_q$.*

(c) *The element $a = b^{p^k}$ is in $\mathcal{U}(p^t)$ and the polynomial $f(x^{p^t})$ has the following factorization in $\mathbb{F}_q[x]$:*

$$f(x^{p^t}) = \prod_{j=0}^{p^t-1} [a^{-mj} g(a^j x)].$$

Remark

If $\langle f(x), n\rangle$ satisfies the reducible condition, where $n = \prod_{i=1}^{u} p_i^{\beta_i}$, then iterating the process for each prime divisor we obtain the n irreducible factors of $f(x^n)$ over $\mathbb{F}_q$.

Example

Consider the irreducible polynomial $f(x) = x^2 - 11x + 1 \in \mathbb{F}_{59}[x]$ of degree 2 and order 12

Example

Consider the irreducible polynomial $f(x) = x^2 - 11x + 1 \in \mathbb{F}_{59}[x]$ of degree 2 and order 12

We are going to find the complete factorization of $f(x^{29^{d+1}})$ for all $d \geq 0$.

Example

Consider the irreducible polynomial $f(x) = x^2 - 11x + 1 \in \mathbb{F}_{59}[x]$ of degree 2 and order 12

We are going to find the complete factorization of $f(x^{29^{d+1}})$ for all $d \geq 0$.

Case $d = 0$: Using the notation of Theorem, we have $r = 12$ and $12s \equiv 1 \pmod{19}$. Then $s = 17$ and we set $l = \frac{rs-1}{29} = 7$.

Example

Consider the irreducible polynomial $f(x) = x^2 - 11x + 1 \in \mathbb{F}_{59}[x]$ of degree 2 and order 12

We are going to find the complete factorization of $f(x^{29^{d+1}})$ for all $d \geq 0$.

Case $d = 0$**:** Using the notation of Theorem, we have $r = 12$ and $12s \equiv 1 \pmod{19}$. Then $s = 17$ and we set $l = \frac{rs-1}{29} = 7$. Now, by quadratic reciprocity law we can prove that $5 \in \mathcal{U}(29) \subset \mathbb{F}_{59}$.

Example

Consider the irreducible polynomial $f(x) = x^2 - 11x + 1 \in \mathbb{F}_{59}[x]$ of degree 2 and order 12

We are going to find the complete factorization of $f(x^{29^{d+1}})$ for all $d \geq 0$.

Case $d = 0$**:** Using the notation of Theorem, we have $r = 12$ and $12s \equiv 1 \pmod{19}$. Then $s = 17$ and we set $l = \frac{rs-1}{29} = 7$. Now, by quadratic reciprocity law we can prove that $5 \in \mathcal{U}(29) \subset \mathbb{F}_{59}$.

Since $A = \begin{pmatrix} 0 & 1 \\ -1 & 11 \end{pmatrix}$ is the companion matrix of $f^*(x)$, from Theorem

$$g(x) = \det(xI - b^s A^l) = \det(xI - 5^{17} A^7)$$

is a factor of $f(x^{29})$.

Example

Consider the irreducible polynomial $f(x) = x^2 - 11x + 1 \in \mathbb{F}_{59}[x]$ of degree 2 and order 12

We are going to find the complete factorization of $f(x^{29^{d+1}})$ for all $d \geq 0$.

Case $d = 0$**:** Using the notation of Theorem, we have $r = 12$ and $12s \equiv 1 \pmod{19}$. Then $s = 17$ and we set $l = \frac{rs-1}{29} = 7$. Now, by quadratic reciprocity law we can prove that $5 \in \mathcal{U}(29) \subset \mathbb{F}_{59}$.

Since $A = \begin{pmatrix} 0 & 1 \\ -1 & 11 \end{pmatrix}$ is the companion matrix of $f^*(x)$, from Theorem

$$g(x) = \det(xI - b^s A^l) = \det(xI - 5^{17} A^7)$$

is a factor of $f(x^{29})$.

Now $A^7 = \begin{pmatrix} 0 & -1 \\ 1 & -11 \end{pmatrix} = -A$ and $5^{17} \equiv 36 \pmod{59}$, therefore

$$g(x) = \det(xI + 23A) = \begin{vmatrix} x & 36 \\ 23 & x - 17 \end{vmatrix} = x^2 - 17x - 2 = x^2 + 42x + 57.$$

Example

Moreover, every monic irreducible factors of $f(x^{29})$ have the form

$$g_j(x) = 5^{-2j} g(5^j x) = 5^{-2j}(25^j x^2 + 42 \cdot 5^j x + 57) = x^2 + (42 \cdot 5^{-j})x + 57 \cdot 5^{-2j}$$

where $j = 0, \cdots, 28$. i.e

$$x^{58} - 11x^{29} + 1 = \prod_{i=0}^{28} (x^2 + 42 \cdot 12^j x + 57 \cdot 26^j).$$

Example

Moreover, every monic irreducible factors of $f(x^{29})$ have the form

$g_j(x) = 5^{-2j} g(5^j x) = 5^{-2j}(25^j x^2 + 42 \cdot 5^j x + 57) = x^2 + (42 \cdot 5^{-j})x + 57 \cdot 5^{-2j}$

where $j = 0, \cdots, 28$. i.e

$$x^{58} - 11x^{29} + 1 = \prod_{i=0}^{28}(x^2 + 42 \cdot 12^j x + 57 \cdot 26^j).$$

Each factor $g_j(x)$ has degree 2 and exponent $12 \cdot 29$. Hence the polynomials $g_j(x^{29^d})$ are irreducible. Therefore

$$f(x^{29^{d+1}}) = \prod_{i=0}^{28}(x^{2 \cdot 29^d} + 42 \cdot 12^j x^{29^d} + 57 \cdot 26^j).$$

Algorithm A.

This algorithm takes as input an irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree m and order e, and p^t a power of a prime.

Algorithm A.

This algorithm takes as input an irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree m and order e, and p^t a power of a prime.

Step A1. Compute $\nu_p(e)$, $\nu_p(q-1)$ and $r := \frac{e}{p_p^{\nu}(e)}$ and verify that $\nu_p(q-1) \geq t + \nu(e)$

Algorithm A.

This algorithm takes as input an irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree m and order e, and p^t a power of a prime.

Step A1. Compute $\nu_p(e)$, $\nu_p(q-1)$ and $r := \frac{e}{p_p^{\nu}(e)}$ and verify that $\nu_p(q-1) \geq t + \nu(e)$

Step A2. Compute $c := x^r \pmod{f(x)}$.

Algorithm A.

This algorithm takes as input an irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree m and order e, and p^t a power of a prime.

Step A1. Compute $\nu_p(e)$, $\nu_p(q-1)$ and $r := \frac{e}{p_p^{\nu}(e)}$ and verify that $\nu_p(q-1) \geq t + \nu(e)$

Step A2. Compute $c := x^r \pmod{f(x)}$.

Step A3. Compute an element b such that $b^{p^t} = c$.

Algorithm A.

This algorithm takes as input an irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree m and order e, and p^t a power of a prime.

Step A1. Compute $\nu_p(e)$, $\nu_p(q-1)$ and $r := \frac{e}{p_p^{\nu}(e)}$ and verify that $\nu_p(q-1) \geq t + \nu(e)$

Step A2. Compute $c := x^r \pmod{f(x)}$.

Step A3. Compute an element b such that $b^{p^t} = c$.

Step A4. Compute s and l such that $rs \equiv 1 \pmod{p^t}$ and $l := \frac{sr-1}{p^t}$.

Algorithm A.

This algorithm takes as input an irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree m and order e, and p^t a power of a prime.

Step A1. Compute $\nu_p(e)$, $\nu_p(q-1)$ and $r := \frac{e}{p_p^{\nu}(e)}$ and verify that $\nu_p(q-1) \geq t + \nu(e)$

Step A2. Compute $c := x^r \pmod{f(x)}$.

Step A3. Compute an element b such that $b^{p^t} = c$.

Step A4. Compute s and l such that $rs \equiv 1 \pmod{p^t}$ and $l := \frac{sr-1}{p^t}$.

Step A5. Compute $\beta = x^{-l} b^s \mod f(x)$.

Algorithm A.

This algorithm takes as input an irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree m and order e, and p^t a power of a prime.

Step A1. Compute $\nu_p(e)$, $\nu_p(q-1)$ and $r := \frac{e}{p_p^{\nu}(e)}$ and verify that $\nu_p(q-1) \geq t + \nu(e)$

Step A2. Compute $c := x^r \pmod{f(x)}$.

Step A3. Compute an element b such that $b^{p^t} = c$.

Step A4. Compute s and l such that $rs \equiv 1 \pmod{p^t}$ and $l := \frac{sr-1}{p^t}$.

Step A5. Compute $\beta = x^{-l} b^s \mod f(x)$.

Step A6. Compute one factor of $f(y)$ as $g_0(y) = (y-\beta)(y-\beta^q)\cdots(y-\beta^{q^{m-1}}) \in \frac{\mathbb{F}_q[x]}{(f(x))}[y]$.

Algorithm A.

This algorithm takes as input an irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree m and order e, and p^t a power of a prime.

Step A1. Compute $\nu_p(e)$, $\nu_p(q-1)$ and $r := \frac{e}{p_p^{\nu}(e)}$ and verify that $\nu_p(q-1) \geq t + \nu(e)$

Step A2. Compute $c := x^r \pmod{f(x)}$.

Step A3. Compute an element b such that $b^{p^t} = c$.

Step A4. Compute s and l such that $rs \equiv 1 \pmod{p^t}$ and $l := \frac{sr-1}{p^t}$.

Step A5. Compute $\beta = x^{-l} b^s \mod f(x)$.

Step A6. Compute one factor of $f(y)$ as $g_0(y) = (y-\beta)(y-\beta^q)\cdots(y-\beta^{q^{m-1}}) \in \frac{\mathbb{F}_q[x]}{(f(x))}[y]$.

Step A7. Pick random elements $\alpha \in \mathbb{F}_q$ until $\alpha^{(q-1)/p} \neq 1$. Then $a := \alpha^{(q-1)/p^t}$ is an element of order p^t.

Algorithm A.

This algorithm takes as input an irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree m and order e, and p^t a power of a prime.

Step A1. Compute $\nu_p(e)$, $\nu_p(q-1)$ and $r := \frac{e}{p_p^{\nu}(e)}$ and verify that $\nu_p(q-1) \geq t + \nu(e)$

Step A2. Compute $c := x^r \pmod{f(x)}$.

Step A3. Compute an element b such that $b^{p^t} = c$.

Step A4. Compute s and l such that $rs \equiv 1 \pmod{p^t}$ and $l := \frac{sr-1}{p^t}$.

Step A5. Compute $\beta = x^{-l} b^s \mod f(x)$.

Step A6. Compute one factor of $f(y)$ as $g_0(y) = (y-\beta)(y-\beta^q)\cdots(y-\beta^{q^{m-1}}) \in \frac{\mathbb{F}_q[x]}{(f(x))}[y]$.

Step A7. Pick random elements $\alpha \in \mathbb{F}_q$ until $\alpha^{(q-1)/p} \neq 1$. Then $a := \alpha^{(q-1)/p^t}$ is an element of order p^t.

Step A8. Compute the other factors of $f(y)$ as $g_j(y) = a^{-jm} g(a^j y)$ for $j = 1, \ldots, p^t - 1$.

Computational Complexity

Taking powers in $\mathbb{F}_q$ and calculating $x^d \pmod{f(x)}$ (Steps A2 and A5)

If $a \in \mathbb{F}_q$, taking squares successively is a well-known fast process for finding a^n in essentially $2\log_2(n)$ products of elements in $\mathbb{F}_q$.

Computational Complexity

Taking powers in $\mathbb{F}_q$ and calculating $x^d \pmod{f(x)}$ (Steps A2 and A5)

If $a \in \mathbb{F}_q$, taking squares successively is a well-known fast process for finding a^n in essentially $2\log_2(n)$ products of elements in $\mathbb{F}_q$.

The product of two polynomials and reduction modulo $f(x)$ can be done with

$$O(m \log m \log \log m)$$

products in $\mathbb{F}_q$ using the fast Euclidean algorithm and the Cantor-Kaltofen Algorithm.

Computational Complexity

Taking powers in $\mathbb{F}_q$ and calculating $x^d \pmod{f(x)}$ (Steps A2 and A5)

If $a \in \mathbb{F}_q$, taking squares successively is a well-known fast process for finding a^n in essentially $2\log_2(n)$ products of elements in $\mathbb{F}_q$.

The product of two polynomials and reduction modulo $f(x)$ can be done with

$$O(m \log m \log \log m)$$

products in $\mathbb{F}_q$ using the fast Euclidean algorithm and the Cantor-Kaltofen Algorithm.

Thus the computation of $x^d \pmod{f(x)}$ when $d > m$ requires

$$O(m \log \frac{d}{m} \log m \log \log m)$$

products in $\mathbb{F}_q$.

Taking roots in $\mathbb{F}_q$ (Step A3)

Taking p-root in a finite field can be computed by means of the Adleman Manders Miller algorithm in

$$O(p\nu_p(q-1)\log^3 q)$$

steps.

Taking roots in $\mathbb{F}_q$ (Step A3)

Taking p-root in a finite field can be computed by means of the Adleman Manders Miller algorithm in

$$O(p\nu_p(q-1)\log^3 q)$$

steps.

Iterating this algorithm, we can solve the equation $x^{p^t} - c = 0$ (or find a primitive p^t-th root of unity when $c = 1$) and the algorithm has complexity

$$O(p^t \log^3 q).$$

Taking roots in $\mathbb{F}_q$ (Step A3)

Taking p-root in a finite field can be computed by means of the Adleman Manders Miller algorithm in

$$O(p\nu_p(q-1)\log^3 q)$$

steps.

Iterating this algorithm, we can solve the equation $x^{p^t} - c = 0$ (or find a primitive p^t-th root of unity when $c = 1$) and the algorithm has complexity

$$O(p^t \log^3 q).$$

In the special case when $t = \nu_p(q-1)$, i.e. $\gcd(p^t, (q-1)/p^t) = 1$, we can use Barreto Voloch algorithm, which has complexity $O(p^t \log\log q \log q)$.

Computation of the minimal polynomial of $\beta \in \mathbb{F}_q[x]/(f(x))$ (Step A6) Using an algorithm of Shoup, the minimal polynomial of β can be computed in

$$O(m^{1.688})$$

operations in $\mathbb{F}_q$.
Note that if $n = p_1^{t_1} \cdots p_i^{t_i}$, we can iterate the algorithm i times, where i is at most $O(\log n)$, hence at most $O(\log q)$.

In conclusion, if $\langle f(x), n\rangle$ satisfies the reducible condition, we find the complete factorization of $f(x^n)$ over $\mathbb{F}_q$ with complexity bounded by

$$O(m \log(M/m) \log m \log\log m \log q + m^{1.688} \log q + n \log^3 q),$$

where $M := \max\{r, l\} < q^m$.

In conclusion, if $\langle f(x), n\rangle$ satisfies the reducible condition, we find the complete factorization of $f(x^n)$ over $\mathbb{F}_q$ with complexity bounded by

$$O(m\log(M/m)\log m\log\log m\log q + m^{1.688}\log q + n\log^3 q),$$

where $M := \max\{r, l\} < q^m$. In the worst case, we have $\log M = O(m\log q)$, and the complexity is bounded by

$$\tilde{O}(m^2\log^2 q + n\log^3 q).$$

In conclusion, if $\langle f(x), n\rangle$ satisfies the reducible condition, we find the complete factorization of $f(x^n)$ over $\mathbb{F}_q$ with complexity bounded by

$$O(m\log(M/m)\log m\log\log m\log q + m^{1.688}\log q + n\log^3 q),$$

where $M := \max\{r, l\} < q^m$. In the worst case, we have $\log M = O(m\log q)$, and the complexity is bounded by

$$\tilde{O}(m^2\log^2 q + n\log^3 q).$$

On other hand, $f(x^n)$ is a polynomial of degree mn such that each of its irreducible factors has degree m, using the probabilistic algorithm of von zur Gathen and Shoup the expected number of operations is

$$O((nm)^{1.688} + (nm)^{1+o(1)}\log q).$$

In conclusion, if $\langle f(x), n\rangle$ satisfies the reducible condition, we find the complete factorization of $f(x^n)$ over $\mathbb{F}_q$ with complexity bounded by

$$O(m\log(M/m)\log m\log\log m\log q + m^{1.688}\log q + n\log^3 q),$$

where $M := \max\{r, l\} < q^m$. In the worst case, we have $\log M = O(m\log q)$, and the complexity is bounded by

$$\tilde{O}(m^2\log^2 q + n\log^3 q).$$

On other hand, $f(x^n)$ is a polynomial of degree mn such that each of its irreducible factors has degree m, using the probabilistic algorithm of von zur Gathen and Shoup the expected number of operations is

$$O((nm)^{1.688} + (nm)^{1+o(1)}\log q).$$

Therefore, our algorithm is faster than the one of von zur Gathen and Shoup in the case where q is not very big ($q < \exp((mn)^{0.5626})$) and the order of growth of n is greater than

$$\tilde{O}(m^{0.185}(\log q)^{1.185}).$$