Chapter 14 Factoring polynomials over finite fields

Three central steps for factorization of univariate polynomials over finite fields:

1. squarefree factorization
2. distinct-degree factorization (99% computing time)
3. equal-degree factorization

14.1 Factorization of polynomials

$\mathbb{Z}$ and $\mathbb{F}[x_1, \ldots, x_n]$ ($\mathbb{F}$ is a field) are Unique Factorization Domains:

1. The Fundamental theorem of number theory states that every integer can be factored uniquely as a product of primes.

2. Any field $\mathbb{F}$ and the polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ can be factored uniquely into product of irreducible polynomials.

A polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ is irreducible if and only $f \notin \mathbb{F}$ and for any $g, h \in \mathbb{F}[x_1, \ldots, x_n]$ with $f = g \cdot h$ we have $g \in \mathbb{F}$ or $h \in \mathbb{F}$. f is squarefree if it has no proper quadratic divisor.

Theorem 1. *Fermat's little theorem For nonzero $a \in \mathbb{F}_q$, we have $a^{q-1} = 1$, and for all $a \in \mathbb{F}_q$, we have $a^q = a$, and*

$$x^q - x = \prod_{a \in \mathbb{F}_q} (x - a) \text{ in } \mathbb{F}_q[x]$$

Theorem 2. *$f \in \mathbb{F}_q[x]$ is irreducible of degree n, then $\mathbb{F}_q[x] / < f >$ is a field with q^n elements.*

14.2 Distinct-degree factorization

Theorem 3. *For any $d \geq 1$, $x^{q^d} - x \in \mathbb{F}_q[x]$ is the product of all monic irreducible polynomials in $\mathbb{F}_q[x]$ whose degree divides d.*

Proof:

1. $x^{q^d} - x = \prod_{a \in \mathbb{F}_{q^d}} (x - a)$ is squarefree.

2. For any monic irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree n that

$$f \text{ divides } x^{q^d} - x \Longleftrightarrow n \text{ divides } d$$

The distinct-degree factorization of a non-constant polynomial $f \in \mathbb{F}_q[x]$ is the sequence $(g_1, g_2, \ldots, g_s)$ of polynomials, where g_i is the product of all monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree i that divide f and $g_s \neq 1$(but some g_i for $i < s$ may be 1).

$$f = g_1 \cdot g_2 \cdots g_s$$

Distinct-degree factorization

Input: A squarefree monic polynomial $f \in \mathbb{F}_q[x]$ of degree $n > 0$.

Output: The distinct-degree decomposition $(g_1, \ldots, g_s)$ of f.

1. $h_0 \longleftarrow x$, $f_0 \longleftarrow f$, $i \longleftarrow 0$
   repeat

2. $i \longleftarrow i + 1$ compute $h_i = h_{i-1}^q$ rem f

3. $g_i \longleftarrow \gcd(h_i - x, f_{i-1})$, $f_i \longleftarrow \frac{f_{i-1}}{g_i}$

4. until $f_i = 1$

5. $s \longleftarrow i$, return $(g_1, \ldots, g_s)$.

Early abort The algorithm stops after $i = \max\{m_1/2, m_2\} \leq n/2$ where m_1 and m_2 are the degrees of the largest and the second largest irreducible factor of f, i.e. $\deg f_i < 2(i+1)$.

Theorem 4. *The distinct-degree factorization algorithm takes $O(sM(n)\log(nq))$ operations in $\mathbb{F}_q$, where s is the largest degree of an irreducible factor of f.*

14.3 Equal-degree factorization: Cantor and Zassenhaus's algorithm

Lemma 1. *Let q be a prime power, k a divisor of $q-1$, and $S = \{b^k : b \in \mathbb{F}_q^\times\}$*

1. *S is a subgroup of order $(q-1)/k$.*
2. *$S = \{a \in \mathbb{F}_q^\times : a^{(q-1)/k} = 1\}$*

Proof: S is the image of $\sigma_k : \mathbb{F}_q^\times \longrightarrow \mathbb{F}_q^\times$ with $\sigma_k(b) = b^k$ and the kernel of σ_k is

$$\ker\sigma_k = \{a \in \mathbb{F}_q^\times : \sigma_k(a) = 1\} = \{a \in \mathbb{F}_q^\times : a^k = 1\},$$

$$q - 1 = \sharp\mathbb{F}_q^\times = \sharp\ker\sigma_k \cdot \sharp\mathrm{im}\sigma_k = \sharp\ker\sigma_k \cdot \sharp S \leq k \cdot (q-1)/k = q - 1$$

Applying the lemma for $k = 2$ and $k = (q-1)/2$, we obtain the following.

Lemma 2. *Let q be an odd prime power and*

$$S = \{a \in \mathbb{F}_q^\times : \exists b \in \mathbb{F}_q^\times \; a = b^2\}$$

be the set of squares in $\mathbb{F}_q^\times$. Then

1. *$S \subseteq \mathbb{F}_q^\times$ is a multiplicative subgroup of order $(q-1)/2$.*

2. *$S = \{a \in \mathbb{F}_q^\times : a^{(q-1)/2} = 1\}$*

3. *$a^{(q-1)/2} \in \{1, -1\}$ for all $a \in \mathbb{F}_q^\times$.*

Suppose $f = f_1 \cdots f_r$ with distinct monic irreducible $f_1, \ldots f_r \in \mathbb{F}_q[x]$ of degree d, assume $r \geq 2$. Since $\gcd(f_i, f_j) = 1$, we have the ring isomorphism

$$\chi : R = \mathbb{F}_q[x]/ < f > \longrightarrow \mathbb{F}_q[x]/ < f_1 > \times \cdots \times \mathbb{F}_q[x]/ < f_r >$$

$\mathbb{F}_q[x]/ < f_i >$ is a field with q^d elements and an algebraic extension of $\mathbb{F}_q$.

$$\mathbb{F}_q \subseteq \mathbb{F}_q[x]/ < f_i > \cong \mathbb{F}_{q^d}$$

For $a \in \mathbb{F}_q[x]$, $f_i | a \iff \chi_i(a) = 0$:

$$\chi(a \mod f) = (a \mod f_1, \ldots, a \mod f_r) = (\chi_1(a), \ldots, \chi_r(a))$$

Let $e = (q^d - 1)/2$, $\epsilon_i = \chi_i(a^e) \in \{1, -1\}$, therefore

$$\chi(a^e - 1) = (\epsilon_1 - 1, \ldots, \epsilon_r - 1)$$

$a^e - 1$ is a splitting polynomial unless $\epsilon_1 = \cdots = \epsilon_r$.

Algorithm 14.8 Equal-degree splitting

Input: A squarefree monic polynomial $f \in \mathbb{F}_q[x]$ of degree $n > 0$, for an odd prime power q, and a divisor d of n, all irreducible factors of f have degree $d < n$.

Output: A proper monic factors $g \in \mathbb{F}_q[x]$ of f or failure.

1. choose $a \in \mathbb{F}_q[x]$ with $\deg a < n$ at random
   if $a \in \mathbb{F}_q$ then return "failure"

2. $g_1 \longleftarrow \gcd(a, f)$, if $g_1 \neq 1$ then return g_1.

3. compute $b = a^{(q^d-1)/2}$rem$f$

4. $g_2 \longleftarrow \gcd(b-1, f)$
   if $g_2 \neq 1$ and $g_2 \neq f$ then return g_2 else return "failure"

Theorem 5. *Algorithm 14.8 works correctly as specified. It returns "failure" with probability less than* $2^{1-r} \leq 1/2$*, where* $r = n/d \geq 2$ *and takes an expected number of* $O(d \log q + \log n)M(n))$ *in* $\mathbb{F}_q$*.*

The usual trick of running the algorithm k times makes the failure probability less than $2^{(1-r)k} \leq 2^{-k}$.

Algorithm 14.10 Equal-degree factorization

Input: A squarefree monic polynomial $f \in \mathbb{F}_q[x]$ of degree $n > 0$, for an odd prime power q, and a divisor d of n, all irreducible factors of f have degree d

Output: The monic irreducible factors of $f \in \mathbb{F}_q[x]$.

1. if $n = d$ then return f

2. call the equal-degree splitting algorithm with input f and d repeatedly until it returns a proper factor $g \in \mathbb{F}_q[x]$ of f.

3. call the algorithm recursively with input g and f/g return the results of the two recursive calls

14.4 A complete factoring algorithm

Algorithm 14.13 Polynomial factorization over finite fields

Input: A nonconstant polynomial $f \in \mathbb{F}_q[x]$ of degree $n > 0$, q is a prime power.

Output: The monic irreducible factors of f and their multiplicities.

1. $h_0 \longleftarrow x, v_0 \longleftarrow \frac{f}{\mathsf{lc}(f)}, i \longleftarrow 0, U \longleftarrow \varnothing$
   repeat

2. $i \longleftarrow i+1$, compute
   $h_i = h_{i-1}^q \mathsf{rem} f$, $g \longleftarrow \gcd(h_i - x, v_{i-1})$

3. if $g \neq 1$ then compute the equal-degree factorization of $g = g_1 \ldots g_s$

4. $v_i \longleftarrow v_{i-1}$
   for $j = 1, \ldots, s$ do
      $e \longleftarrow 0$
      while $g_j | v_i$ do $v_i \longleftarrow \frac{v_i}{g_j}, e \longleftarrow e + 1$
      $U \longleftarrow U \cup \{(g_j, e)\}$

5. until $v_i = 1$

6. return U.

Theorem 6. *Algorithm 14.13 correctly computes the irreducible factorization of f. If $\deg f = n$, then it takes an expected number of $O(nM(n)\log(qn))$ arithmetic operations in $\mathbb{F}_q$.*

Proof: Suppose

$$h_i \equiv x^{q^i} \mod f, v_i = \mathsf{lc}(f) \prod_{\deg f_k > i} f_k^{e_k}$$

We have

$$g = \gcd(h_i - x, v_{i-1}) = \gcd(x^{q^i} - x, v_{i-1}) = \prod_{\deg f_k = i} f_k$$

14.5 Application: root finding

Algorithm 14.15 Root finding over finite fields

Input: A nonconstant polynomial $f \in \mathbb{F}_q[x]$.

Output: The distinct roots of f in $\mathbb{F}_q$.

1. compute $h = x^q \text{rem} f$.

2. $g \longleftarrow \gcd(h - x, f), r \longleftarrow \deg g$
   if $r = 0$ then return $\varnothing$.

3. compute the equal-degree factorization of $g = (x - u_1) \cdots (x - u_r)$,
   return $u_1, \ldots u_r$.

Theorem 7. *Given $f \in \mathbb{F}_q[x]$ of degree n, we can find all roots of f in $\mathbb{F}_q$ using an expected number of $O(M(n) \log n \log(nq))$ operations in $\mathbb{F}_q$.*

14.6 Squarefree factorization

Let $f = \prod_{1 \le i \le r} f_i^{e_i}$ be the irreducible factorization of monic polynomial f. The squarefree part of f to be $\prod_{1 \le i \le r} f_i$, then

$$f' = \sum_{1 \le i \le r} e_i \frac{f}{f_i} f_i'$$

$$f_i^{e_i - 1} | f', f_i^{e_i} \nmid f' \, \text{since} \, f_i \nmid e_i f_i'$$

Algorithm 14.19 Squarefree part in characteristic zero

Input: $f \in \mathbb{F}[x]$ monic of degree $n > 0$ where $\mathbb{F}$ is a field of characteristic zero.

Output: The squarefree part of f.

1. $u \longleftarrow \gcd(f, f')$

2. return $v = \frac{f}{u}$

The squarefree decomposition of $f \in \mathbb{F}[x]$ is

$$f = g_1 g_2^2 g_3^3 \cdots g_m^m$$

where g_i are squrefree and pairwise coprime.

Algorithm 14.21 Yun's Squarefree factorization in characteristic zero

Input: $f \in \mathbb{F}[x]$ monic of degree $n > 0$ where $\mathbb{F}$ is a field of characteristic zero.

Output: The squarefree decomposition of f.

1. $u \longleftarrow \gcd(f, f'), v_1 \longleftarrow \frac{f}{u}, w_1 \longleftarrow \frac{f'}{u}$

2. $i \longleftarrow 1$ repeat
   $h_i \longleftarrow \gcd(v_i, w_i - v_i'), v_{i+1} \longleftarrow \frac{v_i}{h_i}, w_{i+1} \longleftarrow \frac{w_i - v_i'}{h_i}$
   $i \longleftarrow i + 1$ until $v_i = 1$
   $k \longleftarrow i - 1$

3. return $(h_1, \ldots, h_k)$

Lemma 3. *Let $\mathbb{F}$ be a field of characteristic zero, $g_1, \ldots, g_m \in \mathbb{F}[x]$ monic squarefree and pairwise coprime, $g = g_1 \cdots g_m$ and $h = \sum_{1 \le i \le m} c_i g_i' g/g_i$, for some constants $c_i \in \mathbb{F}$. Then $\gcd(g, h - cg') = \prod_{c_j = c} g_j$ for all $c \in \mathbb{F}$.*

Proof: We have $g' = \sum_{1 \le i \le m} g_i' g/g_i$, hence

$$h - cg' = \sum_{1 \le i \le m} (c_i - c) g_i' \frac{g}{g_i}$$

Thus the claim follows from

$$\gcd(g_j, h - cg') = \gcd\left(g_j, (c_j - c) g_j' \frac{g}{g_j}\right) = \gcd(g_j, c_j - c)$$

Theorem 8. *The algorithm uses $O(M(n)\log n)$ operations in $\mathbb{F}$ and it computes correctly the squarefree decomposition of f.*

It can be proved by induction on i that

$$h_i = g_i (i \geq 1), v_{i+1} = \prod_{i<j\leq m} g_j, w_{i+1} = \sum_{i<j\leq m} (j-i) g_j' \frac{v_{i+1}}{g_j}$$

14.8 Algorithms based on linear algebra

Let $f \in \mathbb{F}_q[x]$ be a squarefree monic polynomial of degree $n > 0$ and $R = \mathbb{F}_q[x]/ < f >$. Then R is a vector space of dimension n over $\mathbb{F}_q$, and the map

$$\beta : R \longrightarrow R \text{ with } \beta(a) = a^q - a$$

is F_q-linear.

If $f = f_1 \cdots f_r$ is the irreducible factorization of f, then we have

$$R \cong \mathbb{F}_q[x]/ < f_1 > \times \cdots \times \mathbb{F}_q[x]/ < f_r >,$$

and

$$\mathbb{F}_q[x]/ < f_1 > \cong F_{q^{\deg f_i}} \supset F_q$$

For $a \in F_q[x]$, we have

$$\begin{aligned} a \mod f \in \ker\beta &\iff a^q \equiv a \mod f \\ &\iff a^q \equiv a \mod f_i, 1 \le i \le r \\ &\Longleftarrow a \equiv s_i \mod f_i, s_i \in \mathbb{F}_q, 1 \le i \le r \end{aligned}$$

Thus $\ker\beta$ is a subspace corresponding to $\mathbb{F}_q \times \cdots \times \mathbb{F}_q = \mathbb{F}_q^r$.

The Petr-Berlekamp matrix Q of f representing the Frobenius map $\theta : \theta(a) = a^q$ with respect to the monomial basis $x^{n-1} \mod f, \dots x \mod f, 1 \mod f$ of R.

Theorem 9. *A polynomial* $a(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *satisfies* $a(x)^q \equiv a(x) \mod f(x)$ *if and only if its coefficient vector in the null space of* $Q - I$,

$$f \text{is irreducible} \iff r = 1 \iff \text{rank}(Q - I) = n - 1$$

Algorithm 14.31 Berlkamp's algorithm

Input: A monic squarefree $f \in \mathbb{F}_q[x]$ monic of degree $n > 0$, where q is an odd prime power.

Output: Either an irreducible factor g of f or "failure".

1. compute $x^q \text{rem} f$

2. for $0 \leq i < n$ compute $x^{qi} \text{rem} = \sum_{0 \leq j < n} q_{ij} x^j$
   $Q \longleftarrow (q_{ij})_{0 \leq i,j < n}$

3. use Gaussian elimination on $Q - I \in \mathbb{F}_q^{n \times n}$ to compute the dimension $r \in \mathbb{N}$ and a basis $b_1 \mod f, \ldots, b_r \mod f$ of the $\ker \beta$
   if $r = 1$ then return f

4. choose independent uniformly random elements $c_1, \ldots, c_r \in \mathbb{F}_q$
   $a \longleftarrow c_1 b_1 + \cdots + c_r b_r$

5. $g_1 \longleftarrow \gcd(a, f)$
   if $g_1 \neq 1$ then return g_1

6. compute $b = a^{(q-1)/2}$rem$f$

7. $g_2 \longleftarrow \gcd(b-1, f)$
   if $g_2 \neq 1$ and $g_2 \neq f$ then return g_2 else return "failure"

Theorem 10. *Algorithm 14.31 works correctly as specified and fails with probability at most $1/2$. It uses $O(n^\omega + M(n)\log q)$ operations in F_q if $\omega > 2$.*

14.9 Testing irreducibility and constructing irreducible polynomials

Corollary 1. *A polynomial $f \in \mathbb{F}_q[x]$ of degree $n \geq 1$ is irreducible if and only if*

1. *f divides $x^{q^n} - x$ and*

2. *$\gcd(x^{q^{n/t}} - x, f) = 1$ for all prime divisors t of n*

Algorithm 14.36 Irreducibility test over finite fields

Input: $f \in \mathbb{F}_q[x]$ of degree n

Output: "irreducible" or "reducible"

1. compute $x^q \text{rem} f$ and $a = x^{q^n} \text{rem} f$
   if $a \neq x$ then return "reducible"

2. for all prime divisors t of n do

3. compute $b = x^{q^{n/t}} \text{rem} f$
   if $\gcd(b - x, f) \neq 1$ then return "reducible"

4. return "irreducible"

Theorem 11. *Algorithm 14.36 correctly decides whether the input polynomials is irreducible. It can be implemented so as to use* $O(M(n)\log q + (n^{(\omega+1)/2} + n^{1/2}M(n)\delta(n)\log n)$ *operations in* $\mathbb{F}_q$

Lemma 4. *Let* q *be a prime power and* $n \in \mathbb{N}_{\geq 1}$*. then the number* $I(n,q)$ *of monic irreducible polynomials of degree* n *in* $\mathbb{F}_q[x]$ *satisfies*

$$\frac{q^n - 2q^{n/2}}{n} \leq I(n,q) \leq \frac{q^n}{n}$$

In particular, if $q^n \geq 16$*, then the probability* p_n *for a uniformly random monic polynomial of degree* n *to be irreducible satisfies*

$$\frac{1}{2n} \leq \frac{1}{n}\left(1 - \frac{2}{q^{n/2}}\right) \leq p_n \leq \frac{1}{n}$$