Lecture 9: Factoring in $\mathbb{F}_q[x]$

Algorithmic Number Theory (Fall 2014)
Rutgers University
Swastik Kopparty
Scribe: Katie McKeon

1 Overview

Throughout this lecture, we assume that q is a power of an odd prime p and f is a polynomial of degree d which we wish to factor in the field $\mathbb{F}_q[x]$. We will give a randomized algorithm running in $poly(d, \log q)$ time which gives the correct factorization with high probability. Our method can be summarized as follows.

Algorithm 1 Factor $f(x) \in \mathbb{F}_q[x]$

1. Reduce to the case that $f(x)$ is square free.
2. Reduce to the case that all irreducible factors have the same degree.
3. Factor a square free polynomial with all irreducible factors in $\mathbb{F}_q[x]$ having the same degree.

2 Preprocessing the Polynomial

Given $f(x) \in \mathbb{F}_q[x]$ of degree d, we now discuss steps 1 and 2 of Algorithm 1.

2.1 Reduction to Square Free Polynomials

Recall from the last lecture that if $f(x)$ is not square free, then one of the following is true:

i. The degree of $\gcd(f(x), f'(x))$ is in $[1, d-1]$. In the last lecture, we discussed how to find a factor of f in this case.

ii. $f'(x) = 0$ and $f(x)$ is a perfect pth power. In other words, $f(x) = g(x^{p^m})$ for some polynomial g and $m \geq 1$. In this case, we can factor g.

2.2 Reduction to Irreducible Factors of the Same Degree

Student suggestion: Why don't we take two random $a, b \in \mathbb{F}_q$ and find $\gcd(f(ax+b), x^{\frac{q-1}{2}} - 1)$? The hope is that there is a decent chance that the roots of $f(ax+b)$ have nontrivial gcd.

However, if $f(x)$ is ireeduible of degree c, then the roots of f lie in $\mathbb{F}_{q^c}$ and the roots of $x^{\frac{q-1}{2}} - 1$ lie in $\mathbb{F}_q$ (i.e. they are exactly the quadratic residues.) So, this works only if f splits in $\mathbb{F}_q$. This suggests the necessity of breaking f up into factors which contain irreducibles of common degree.

Recall the following fact for finite fields: Let $\mathcal{C}_l$ represent the collection of monic polynomials in $\mathbb{F}_q[x]$ of degree l. Then for any d

$$x^{q^d} - x = \prod_{l|d} \prod_{p \in \mathcal{C}_l} p(x)$$

In particular, $x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha)$

Proof. For all irreducible $p(x) \in \mathbb{F}_q[x]$ whose degree l divides d, the roots of $p(x)$ are in $\mathbb{F}_{q^l} \subseteq \mathbb{F}_{q^d}$. Since the roots of $x^{q^d} - x$ give the field $\mathbb{F}_q^d$, we have that $p(x)$ divides $x^{q^d} - x$.

On the other hand if the degree l of $p(x)$ does not divide d, then a root of $p(x)$ generates $\mathbb{Z}_{q^l} \not\subseteq \mathbb{F}_{q^d}$. Since $x^{q^d} - x$ has derivative -1 it is square free and no powers of p show up in the factorization of $x^{q^d} - x$. □

So, to reduce f into irreducibles of common degree, we initialize $f_1(x) = f(x)$. If $f(x) = \prod_j p_j(x)$ with each p_j irreducible, then we want $f_i(x) = \prod_{j, \deg(p_j) \geq i} p_j(x)$ and $g_i = \prod_{j, \deg(p_j) = i} p_j(x)$ for each i. To find these g_i's and f_i's, let $g_i(x) = \gcd(x^{q^i} - x, f_i(x))$ and $f_{i+1} = f_i(x)/g_i(x)$. Then each g_i is composed of irreducibles of degree exactly i and $f(x) = \prod_i g_i(x)$ and it suffices to factor each g_i. Note that we can find the gcd of $x^{q^i} - x$ and $f_i(x)$ using the algorithm from lecture 8. It is necessary for f to be square free in this step because each factor of $x^{q^i} - x$ occurs only once and therefore the gcd might miss some factors for a particular g_i.

3 Factoring the Preproccessed Polynomial in $\mathbb{F}_q[x]$

Now, we assume that steps 1 and 2 in Algorithm 1 have been completed so that f has all factors of degree l and is squarefree. Then f divides $x^{q^l} - x$ and $x^{q^l} - x = x(x^{\frac{q^l-1}{2}} - 1)(x^{\frac{q^l-1}{2}} + 1)$. Part 3 of the algorithm involves two steps:

1. Pick $r(x) \in \mathbb{F}_q[x]$ of degree $k \geq 2l$ uniformly at random
2. Compute $\gcd(r(x)^{\frac{q^l-1}{2}} - 1, f(x))$. If nontrivial, then we found a factor of f in $\mathbb{F}_q$.

Note that our old algorithm for factoring a polynomial of degree l assumes we can work with $\mathbb{F}_{q^l}$ and gives roots in $\mathbb{F}_{q^l}$. Since we want roots in $\mathbb{F}_q[x]$, and do not need to construct the whole field $\mathbb{F}_{q^l}$, we choose the randomized $r(x)$ and raise it to the power $\frac{q^l-1}{2}$.

Theorem 1. *If f is square free and all its irreducible factors have degree l, then suppose f_1 and f_2 are two irreducible factors of f. Then* $\mathbf{Prob}[f_i(x) | r(x)^{\frac{q^l-1}{2}} - 1] \approx 1/2$ *for each x and $i = 1, 2$.*

Note that for $i = 1, 2$, $f_i(x)$ divides $r(x)^{\frac{q^l-1}{2}} - 1$ if and only if $f_i(x)$ divides $(r(x) - 1 \mod f_i(x))^{\frac{q^l-1}{2}} - 1$ which is a polynomial of degree at most $l - 1$ that we will show is uniformly random.

The idea of this proof is that choosing a uniformly random integer in $[1, 100]$ gives a uniform distribution of remainders $\mod 5$, i.e. the probability that a uniform randomly chosen r has remainder $2 \mod 5$ is $1/5$.

Proof. Write $r(x) = b(x)f_i(x) + u_i(x)$ for $i = 1, 2$, i.e. $u_i \equiv r \mod f_i$. Observe that

$$\mathbf{Prob}[f_i(x)|u_i(x)^{\frac{q^l-1}{2}} - 1] = \mathbf{Prob}[u_i(x)^{\frac{q^l-1}{2}} \equiv 1 \text{ in } \mathbb{F}_q[x]/\langle f_i(x)\rangle] = \mathbf{Prob}[u_i(\alpha_i)^{\frac{q^l-1}{2}} - 1 = 0 \text{ in } \mathbb{F}_{q^l}] = 1/2$$

where α_i is a root of f_i in $\mathbb{F}_{q^l}$. By the Chinese Remainder Theorem, specifying a remainder mod f_1 and mod f_2 is the same as specifying a remainder in $f_1 \cdot f_2$ because f_1 and f_2 are relatively prime (as both are irreducible and f was square free.) Therefore, the remainders u_1 and u_2 are uniform and independent. Since

$$\mathbf{Prob}[f_1|r(x)^{\frac{q^l-1}{2}} - 1 \text{ and } f_2|r(x)^{\frac{q^l-1}{2}} - 1] = \mathbf{Prob}[u_1(\alpha_1) \in QR \text{ and } u_2(\alpha_2) \in QR]$$

(where QR denotes the set of quadratic residues in $\mathbb{F}_{q^l}$), we have that the probability above is $1/4$. Similarly, the probability that f_1 divides $r(x)^{\frac{q^l-1}{2}} - 1$ and f_2 does not is $1/4$ and vice versa. So,the probability that the GCD will be nontrivial, i.e. one of f_1 or f_2 divides $r(x)^{\frac{q^l-1}{2}} - 1$, is $1/2$. □

4 Analysis

Theorem 1 gives a high probability that step three will produce a factor of f, if f factors. We can easily check whether f factors because, a polynomial $f(x)$ of degree d irreducible if and only if $\gcd(x^{q^l} - x, f(x)) = 1$ for all $l < d$. So, checking whether the factors we found are irreducible amounts to more gcd operations.

Recall that an efficient method for computing $\gcd(x^{\frac{q^l-1}{2}} - 1, g(x))$ was given a previous lecture. Namely, compute $x \mod g(x); x^2 \mod g(x); x^4 \mod g(x); \ldots; x^{2^{\log q}} \mod g(x)$ sequentially and reduce at each step. This runs in $\texttt{poly}(l \log q)$ time. Thus, Algorithm 1 which uses this gcd operation (with $l \leq n$) runs in $\texttt{poly}(d, \log q)$ time.

Note that this algorithm cannot be adjusted in a minor way to give a deterministic algorithm for finding factors. This was not even possible in the previous algorithm for finding quadratic residues. However, next time we will see an algorithm of Berlekemp which runs in time $\texttt{poly}(d, p, \log q)$ which is deterministic.

Recall that throughout we assumed that q was a power of an odd prime. On the other hand, if $p = 2$, we use the polynomial

$$(x + x^2 + x^4 + \ldots + x^{2^{n-1}})$$

throughout the algorithm instead of $x^{\frac{q^l-1}{2}} - x$. This is a sparse polynomial with about half of $_{2^n}$ being roots of the polynomial.