6.S897 Algebra and Computation Feb 23, 2015

Lecture 7

Lecturer: Madhu Sudan *Scribe: David J. Rosenbaum*

Last lecture, we showed how to find the linear factors of a polynomial and sketched the algorithm for finding irreducible factors of degree larger than 1. Let $f \in \mathbb{F}_q$ be a monic polynomial of degree n where $q = p^s$. (The assumption that f is monic is of course WLOG.) In this lecture, we'll show the following:

1. A randomized algorithm for factoring f in $\text{poly}(n, \log q)$ expected time.
2. A deterministic algorithm for factoring f in $\text{poly}(n, p, s)$. (This is efficient if the characteristic p is small.)

First, we mention an open problem that illustrates the difficulty of handling fields of large characteristic in deterministic factoring algorithms.

Open problem 1
Given: *$a \in \mathbb{Z}_p$ where p is prime*
Find: *b such that $b^2 = a \pmod p$ deterministically in $\text{polylog}(p)$ time*

This can be done assuming the Generalized Riemann Hypothesis but it is open to accomplish this unconditionally.

In this lecture, we'll focus only on obtaining polynomial time algorithms for factoring but won't worry about the exponent. Thus, we can think of the problem of factoring $f \in \mathbb{F}_q[x]$ as finding polynomials $g, h \in \mathbb{F}[x]$ with $\deg f, \deg h \geq 1$ such that $f = gh$.

1 Randomized factoring

The randomized factoring algorithm works as follows:

1. Check for repeated factors
   If $f' = 0$, then $f = \sum_{i=0}^{k} c_k x^{ip}$ where $kp \leq n$. In this case, $f^{1/p} = \sum_{i=0}^{k} c_k^{1/p} x^i$ divides f and is neither constant nor a multiple of f. (Recall from the last lecture that p^{th} roots exist in a field of characteristic p.) In this case, we output $(f^{1/p}, f/f^{1/p})$.

   If $f' \neq 0$ but $g = \gcd(f, f') \neq 1$, we output $(g, f/g)$.

2. Distinct degree factorization
   For each $d = 1, \ldots, n$, if $g = \gcd(f, x^{q^d} - x) \notin \{1, f\}$ then output $(g, f/g)$. The polynomial $x^{q^d} - x$ is divisible by all irreducible polynomials of degree d, so this step pulls out all the irreducible factors of degree d.

3. All irreducible factors of f have degree d (note that we know d from step 2) Pick $h \in \mathbb{F}_q[x]$ of degree $2d-1$ uniformly at random. If $g = \gcd(f, h^{(q^d-1)/2}-1) \notin \{1, f\}$, we output $(g, f/g)$.

We already justified steps 1 and 2 in the previous lecture, so we just need to justify step 3. First, we note that in fields of characteristic 2, we of course cannot divide by 2; in this case, we use $\mathrm{tr}(h)$ instead.

We need to show that $\gcd(f, h^{(q-1)/2} - 1) \notin \{1, f\}$ with high probability. Suppose $f = g_1 \cdots g_k$ where the g_i are distinct monic irreducible polynomials. By the Chinese Remainder Theorem, the mapping

$$\phi : \mathbb{F}_q[x]/\langle f\rangle \to (\mathbb{F}_q[x]/\langle g_1\rangle)\times\cdots\times(\mathbb{F}_q[x]/\langle g_k\rangle) : a \bmod f \mapsto (a \bmod g_1, \ldots, a \bmod g_k)$$

is an isomorphism. Applying this isomorphism to the polynomial $a = h^{(q^d-1)/2}$, we see that the i^{th} component of $\phi(a)$ is zero with probability roughly $1/2$. This follows from the fact that $h \bmod g_i$ is simply an element of the field $\mathbb{F}_q[x]/g_i$ and the zeros of the polynomial a are the quadratic residues of $\mathbb{F}_q[x]/g_i$. Therefore, with probability roughly $1/4$, the first component of $\phi(h)$ is zero and the second component is nonzero. In this case, $g = \gcd(f, h^{(q^d-1)/2}-1) \notin \{1, f\}$ as desired. We can therefore simply keep choosing random polynomials h in step 3 until we obtain such a gcd g.

2 Deterministic factoring

Let $q = p^s$ and let $f \in \mathbb{F}_q[x]$ be the degree n monic polynomial we wish to factor. For deterministic factoring, we seek a polynomial h such that

$$h^p - h \bmod f = 0$$

Two obvious solutions are $h = f$ and $h \in \mathbb{F}_p$ which do not help. We exclude these by requiring that $1 \le \deg h < n$.

First, we show that finding such an h allows us to divide f into a product of smaller polynomials. Recall that

$$h^p - h = \prod_{\alpha\in\mathbb{F}_p} (h - \alpha)$$

Then if $f \mid h^p - h$, there exists $\alpha \in \mathbb{F}_p$ such that $\gcd(f, h - \alpha) \notin \{1, f\}$. Thus, finding such an h is indeed sufficient to factor f. We now turn to the question of whether such an h exists.

Let $f = g_1 \cdots g_k$ where each g_i is a distinct irreducible polynomial of degree d. Now, the Chinese Remainder Theorem implies that there exist $\alpha_1 \neq \alpha 2 \in \mathbb{F}_p$ and a polynomial h such that $h \bmod g_1 = \alpha_1$ and $h \bmod (g_2 \cdots g_k) = \alpha_2$. Since $\alpha^p = \alpha$ for all $\alpha \in \mathbb{F}_p$, we see that this h satisfies $h^p - h = 0$. Moreover, $\deg(h \bmod f) \neq 0$ since $\alpha_1 \neq \alpha_2$ and $\deg h \bmod f < n$.

Now that we've shown existence, we show that we can compute such an h efficiently. It is easy to see that all the h such that $h^p - h = 0$ form a vector space over $\mathbb{F}_p$. We start by representing h as

$$h = \sum_{i=0}^{n-1} c_i x^i$$

Letting $\beta_1, \ldots, \beta_s$ be an $\mathbb{F}_p$-basis for $\mathbb{F}_q$, we write

$$c_i = \sum_{j=1}^{s} c_{ij}\beta_j$$

for each i. Thus, we can express h as a linear function of the c_{ij}'s. Now,

$$h^p = \sum_{i=0}^{n-1} c_i^p x^{ip}$$

and

$$\begin{aligned} c_i^p &= \left(\sum_{j=1}^{s} c_{ij}\beta_j\right)^p \\ &= \sum_{j=1}^{s} c_{ij}^p \beta_j^p \\ &= \sum_{j=1}^{s} c_{ij}\beta_j^p \\ &= \sum_{j,k=1}^{s} c_{ij}\delta_{jk}\beta_k \end{aligned}$$

where $\beta_j^p = \sum_{k=1}^{s} \delta_{jk}\beta_k$. Expanding the equation

$$f \cdot g = h^p - h$$

where $g = \sum_{i=0}^{p(n-1)} d_i x^i$, $d_i = \sum_{i=1}^{s} d_{ij}\beta_j$ and equating the coefficients of the corresponding monomials yields a system of $\mathbb{F}_p$-linear equations in the unknowns c_{ij} and d_{ij} which we can solve in polynomial time.

3 A general idea

The following is a general strategy for factoring:

1. Obtain information about one factor
2. Convert this information into the factor

We can use this idea to show that factorization of $f \in \mathbb{F}_q[x]$ into degree d factors reduces to root finding in $\mathbb{F}_{q^d}$.

Definition 1 *Let $\alpha \in \mathbb{F}_{q^d}$. The minimal polynomial of α in $\mathbb{F}_q[x]$ is the monic polynomial g of minimal degree such that $g(\alpha) = 0$.*

Clearly, every minimal polynomial is irreducible in $\mathbb{F}_q[x]$. (Otherwise, α would be a root of one of its factors.) Moreover, we can find minimal polynomials using linear algebra.

If α is a root of f in $\mathbb{F}_{q^d}$, then $x - \alpha$ divides the minimal polynomial of α.