6.966 Algebra and Computation	September 28, 1998
Lecture 6	
Lecturer: Madhu Sudan	*Scribe: Zulfikar Ramzan*

1 Introduction

In this lecture we covered Berkelamp's Algorithm for factoring polynomials and we also dicussed some properties of irreducible polynomials over finite fields. As an aside, during the last lecture, the algorithm covered was due to Cantor and Zassenhaus. Knuth Volume 2 and the text by Cohen are good references.

2 Berkelamp's Factoring Algorithm

In this section we describe Berkelamp's Factoring Algorithm. It is one of the older algorithms for factoring polynomials, and it's very fundamental. In this lecture, we cover the deterministic variant of the algorithm, which was developed in 1969. This variant has running time polynomial in the degree of the polynomial and in the field size. A randomized version of the algorithm was developed in 1970, but we won't be discussing it during this lecture.

2.1 Main Idea

Say we are given a polynomial $f(x)$, and we need to find $f_1(x), \ldots, f_k(x)$ such that $f(x) = f_1(x)f_2(x)\cdots f_k(x)$. As in Lecture 5, we first reduce to the case where all the f_i's are irreducible, distinct, and of degree d. We work over the field $F = GF(q)$ where $q = p^m$ for some prime p. For conceptual simplicity, we restrict ourselves to the case $k = 2$.

The key idea of the algorithm is to find a polynomial $g \in F[x]$ such that $g(x)^q = g(x) \pmod{f(x)}$, with $0 < \deg(g) < \deg(g)$. This polynomial will turn out to have useful properties which enable us to find non-trivial factors of $f(x)$. We must answer the following questions:

1. Why is finding such a polynomial $g(x)$ useful?
2. Does such a polynomial always exist?
3. If it does exist, how do we find it?

2.2 Usefulness of Finding Such a Polynomial

Consider the polynomial $z^q - z$. Observe that:

$$z^q - z = \prod_{\alpha \in F} (z - \alpha)$$

Similiarly:

$$g(x)^q - g(x) = \prod_{\alpha \in F} (g(x) - \alpha)$$

Since $g(x)^q = g(x) \bmod f(x)$, it follows that $f(x) | g(x)^q - g(x)$. Now if $\underline{0 < \deg(g) < \deg(f)}$ we can exploit our knowledge of the factorization of $g(x)^q - g(x)$ to help factor f. In particular we observe there must be an $\alpha \in F$ such that $gcd(f(x), g(x) - \alpha) \neq 1$. And this greatest common divisor will give you a non trivial factor of $f(x)$. Notice that it was important for us to impose the restriction that $0 < \deg(g) < \deg(f)$. For example, if g was a constant, then $g^q - g = 0$ which is not too useful. Also, if $g(x) = f(x)$ you gain nothing useful.

Now, if we run through all $\alpha \in F$, and take gcd's, we can obtain a non-trivial factorization of $f(x)$. All that remains is to show that the polynomial $g(x)$ exists and we can find it efficiently.

2.3 Showing Existence of Such a Polynomial

To show existence of a polynomial $g(x)$ satisfying the previously mentoined constraints, we make use of the Chinese Remainder Theorem for polynomials. Consider the polynomial $g(x) \bmod f(x)$. We can view this polynomial in terms of the factors $f_1(x), f_2(x)$ of $f(x)$. In particular, we have $(g(x) \bmod f_1(x))$ and $(g(x) \bmod f_2(x))$. And it follows that $g(x)^q = g(x) \bmod f_1(x)$ and $g(x)^q = g(x) \bmod f_2(x)$

So, one approach to constructing $g(x)$ might be to set it equal to constants modulo $f_1(x)$ and $f_2(x)$. In particular, for two constants a, b we let $g(x)$ be the polynomial which satisfies: $g(x) = a \bmod f_1(x)$ and $g(x) = b \bmod f_2(x)$. After fixing a, b we can construct $g(x)$ using the Chinese remainder theorem in the usual way and since a, b are constants, we have $g(x)^q = a^q = a = g(x) \bmod f_1(x)$. Similarly we find $g()^q = g(x) \bmod f_2(x)$ and thus $g(x)^q = g(x) \bmod f(x)$.

Of course this is not useful if g turns out to be a constant, but it is easy to see that there are non-constant polynomials g satisfying this property. To see this, consider all possible pairs $a, b \in F$; Using all such pairs, we can construct q^2 distinct polynomials g, satisfying $g(x)^q = g(x) \bmod f(x)$, all of which have degree less than f. Of these polynomials, only q of them turn out to be a constant polynomial (and this happens whenever $a = b$). So, there are $q^2 - q$ polynomials which have degree greater than 0, but still have a smaller degree than $f(x)$. We can take $g(x)$ to be any one of these polynomials. So, we've now shown that there is a polynomial $g(x)$ satisfying the constraints specified earlier. Unfortunately, we can't use this Chinese Remainder Technique for actually constructing g. Why not? Because in order to construct g via the Chinese Remainder Theorem, we would already need to know $f_1(x)$ and $f_2(x)$ – and these are the polynomials that we've been trying to find in the first place!

2.4 Constructing Such a Polynomial

We've shown that there exists a polynomial g which satisfies $g(x)^q = g(x) \bmod f(x)$ with $0 < \deg(g) < \deg(f)$. Now we show how to construct such a polynomial efficiently. We make the following observation:

Observation 1 *The space of all polynomials $g(x)$ satisfying $g(x)^q = g(x) \bmod f(x)$ is a linear space. In particular, if $g_1(x)^q = g_1(x) \bmod f(x)$ and $g_2(x)^q = g_2(x) \bmod f(x)$ then $(g_1(x) + g_2(x))^q = (g_1(x) + g_2(x)) \bmod f(x)$.*

Proof
$(g_1(x) + g_2(x))^q \bmod f(x)$
$= g_1(x)^q + g_2(x)^q +$ multiples of p
$= g_1(x) + g_2(x) \bmod f(x)$. ■

Since we are looking at a linear space, we can find a basis for the set of all possible g's that work. In particular, suppose $g(x) = g_0 + g_1 x + \ldots + g_l x^l$. First we observe that $g(x)^q = g(x^q)$ and $g(x)^q = (\sum_i g_i x^i)^q = (\sum_i g_i^q x^{iq}) +$ multiples of p $= \sum g_i x^{iq} = g(x^q)$. Now, let's look at $x^{iq} \bmod f$. We can find values α_{ij} such that: $x^{iq} \bmod f = \sum_j \alpha_{ij} x^j (\bmod f)$. So if we have $g(x)^q = g(x) \bmod f$ then:

Since $g(x) = g(x)^q = g(x^q)$, it follows that

$$\sum_{i=0}^{l} g_i \sum_{j=0}^{l} \alpha_{ij} x^j = \sum_{i=0}^{l} g_i x^i$$

And we can find the basis for the set of all solutions.

2.5 Summary of Berkelamp's Factoring Algorithm

The following summarizes the steps needed in order to obtain a non-trivial factor of a polynomial $f(x)$ of degree d over the field $F = GF(q)$ in time $poly(d, q)$ (where $q = p^k$ for some prime p).

Input: A polynomial $f(x)$ defined over the field $F = GF(q)$.
Output: A non trivial factor $h(x)$

1. Obtain a polynomial $g(x)$ satisfying:
   (a) $0 < \deg(g(x)) < \deg(f(x))$
   (b) $g(x)^q = g(x) \bmod f(x)$
2. **for** all elements $\alpha \in F$ **do**:
   (a) let $h(x) \leftarrow gcd(f(x), g(x) - \alpha)$
   (b) **if** $h(x) \neq 1$ **then** output $h(x)$ and terminate.

3 Properties of Irreducible Polynomials

We now shift gears and talk about various properties of irreducible polynomials. Specifically, our goal is to demonstrate that there are many irreducible polynomials of degree d over $GF(q)$. We are also going to find out which irreducible polynomials divide $x^{q^d} - x$, since we needed this for the factoring algorithms. In particular, we show that:

1. For every prime $q = p^k$ and every integer $d > 0$, there exists an irreducible polynomial of degree d over $F = GF(q)$.
2. The probability that a monic polynomial over $GF(q)$ is irreducible is approximately equal to $1/d$.

In order to show these results, we make use of two algebraic concepts. The first is the concept of a Field Extension as a Vector Space, and the second is the Splitting Field of a Polynomial.

3.1 Field Extensions as Vector Spaces

Consider a Field K with a subfield F. Then K can be viewed as a vector space over F. In particular, there are elements $\alpha_1 \ldots \alpha_n \in K$ such that $\sum \lambda_i \alpha_i \neq 0$ for all $\lambda_1, \ldots, \lambda_n \in F$ with $(\lambda_1, \ldots, \lambda_n) \neq (0, \ldots, 0)$. You can think of $\lambda_1, \ldots, \lambda_n$ as a vector in some n-dimensional space over F (with the usual properties); namely, every element in K can be expressed as a linear combination of elements of $\alpha_1, \ldots, \alpha_n$ over F. Moreover, we can define the dimension of K over F (denoted $[K : F]$) as n – where n is the maximum number satisfying the above contraint that $\sum \lambda_i \alpha_i \neq 0$ for all $\lambda_1, \ldots, \lambda_n \in F$ with $(\lambda_1, \ldots, \lambda_n) \neq (0, \ldots, 0)$.

Proposition 2 *If* $[K : F] = n$ *then* $|K| = |F|^n$.

Proof Suppose there exist $\lambda_1, \ldots, \lambda_n$ and $\lambda'_1, \ldots, \lambda'_n$ such that $\sum \lambda_i \alpha_i = \sum \lambda'_i \alpha_i$ where $(\alpha_1, \ldots, \alpha_n) \neq (0, \ldots, 0)$ then $\sum (\lambda_i - \lambda'_i)\alpha_i = 0$ which implies that $\lambda_i = \lambda'_i$. Since there are $|F|^n$ choices of $\lambda_1, \ldots, \lambda_n$ all of which yeild distinct elements under a linear combination with $\alpha_1, \ldots, \alpha_n$, it follows that there are $|F|^n$ elements in K. ∎

Proposition 3 *If* K, L, F *are fields such that* $K \supseteq L \supseteq F$, *then* $[K : F] = [K : L] \cdot [L : F]$.

Proof Suppose $\alpha_1, \ldots \alpha_n$ are a generating set for the extension of K over L, and suppose $\beta_1, \ldots, \beta_m$ are a generating set for the extension of L over F. Then, $\alpha_i \beta_j$ form a generating set for K over F, and they are linearly independent – which proves the proposition. ∎

Exercise 4 *As an exercise, you can try: Given* $Ax = b$ *with* A, b *from* $GF(p^k)$, *find a vector* $x \in GF(p)^n$ *such that* $Ax = b$ *if such a vector exists.*

3.2 Splitting Field of a Polynomial

In this section we define the notion of a *Splitting Field* and prove the existence of a splitting field for any polynomial over a field.

Definition 5 *Given a polynomial $f(x) \in F[x]$, a field extension K of F (i.e. $K \supseteq F$ and K is itself a field) is said to be a splitting field if $f(x)$ splits into linear factors over K (but not over any proper subfield of K).*

Lemma 6 *Every polynomial $f(x) \in F[x]$ has a splitting field.*

Proof Consider an irreducible factor $f_1(x)$ of $f(x)$ where $f_1(x)$ has degree greater than 1 (if none exist, then all factors are linear and we are trivially done). Let $K_1 = F[u]/(f_1(u))$. Then there is an element $u \in K_1$ such that $f_1(u) = 0$ (when we look at $f_1(x) \in K_1[x]$). Therefore, $(x-u)|f_1(x)$ which implies that $(x-u)|f(x)$ (again, we are looking at these polynomials over the field K_1). Now, let $f_2(x) = f(x)/f_1(x)$. Inductively apply the above construction to $f_2(x)$ and K_1. This yields a splitting field. ■

3.3 Existence of Extension Fields of size q^d extending $GF(q)$

We now prove the following theorem regarding the existence of extension fields of size q^d which extend $GF(q)$:

Theorem 7 *For all $q = p^k$ where p is a prime, and for all d, there exists a field of size q^d extending $GF(q)$.*

Proof Consider the splitting field of $x^{q^d} - x$ over $GF(q)$. Call this splitting field K. Now, consider the set $S = \{\alpha \in K \text{ such that } \alpha^{q^d} - \alpha = 0\}$. We claim S satisfies the conditions of the theorem. We need to show that:

1. S is a field.
2. $|S| = q^d$

To see that S is a field, it suffices to check that for all $\alpha, \beta \in S$, $\alpha + \beta, \alpha \cdot \beta, -\alpha, \alpha^{-1} \in S$ – which is fairly straightforward:

1. $(\alpha + \beta)^{q^d} = \alpha^{q^d} + \beta^{q^d} +$ multiples of p $= \alpha^{q^d} + \beta^{q^d} = \alpha + \beta$. Therefore, $\alpha + \beta \in S$.
2. $(\alpha \cdot \beta)^{q^d} = \alpha^{q^d} \cdot \beta^{q^d} = \alpha \cdot \beta$. Therefore, $\alpha \cdot \beta \in S$.
3. $(-\alpha)^{q^d} = -1^{q^d} \cdot \alpha^{q^d} = -1^{q^d} \cdot \alpha = -\alpha$. The last equality follows from the previous one because q^d is odd whenever q is odd, and q is even only if the underlying prime p is 2, in which case, $-1 = 1$ for that field. Therefore, $-\alpha \in S$.
4. $(\alpha^{-1})^{q^d} = (\alpha^{q^d})^{-1} = \alpha^{-1}$. Therefore, $\alpha^{-1} \in S$.

To compute the cardinality of S observe that S cannot have more than q^d elements since $x^{q^d} - x$ has at most q^d roots (since its degree is q^d). Moroever, if you compute $gcd(f, f')$ we see that there are no multiple roots (hence S has at least q^d roots). Specifically, $gcd(f, f') = gcd(x^{q^d} - x, -1) = 1$. We know from a previous lecture that if any polynomial and it's derivative have a greatest common divisor of 1, then the polynomial does not have multiple roots. So, we have shown that S has exactly q^d elements. ■

3.4 Number of Monic Irreducible Polynomials of Degree d

We now show some theorems regarding the number of irreducible polynomials over a field F:

Theorem 8 *There are at least $(q^d-1)/d$ monic irreducible polynomials of degree at most d over $GF(q)$.*

Proof Consider the unique extension field K of F where $|K| = q^d$. Now, for all non zero elements $\alpha \in K$ we form the sequence $\alpha^0, \alpha^1 \ldots, \alpha^l$ where l is chosen to be smallest element such that there exist $\lambda_0, \lambda_1, \ldots, \lambda_l \in F$ with $\sum \lambda_i \alpha_i = 0$ and $(\lambda_0, \lambda_1, \ldots \lambda_l) \neq (0, 0, \ldots, 0)$. We know that $l \leq d$ because K has dimension d. Now, we can restrict $\lambda_l = 1$ because the last term is always non-zero, and we can divide out. Therefore, $f(x) = \sum_{i=0}^{l} \lambda_i x^i$ has degree at most d. Moreoever, $f(\alpha) = 0$. We claim that $f(x)$ is irreducible over $F[x]$. This follows from the fact that if $f(x)$ splits, then we can find a smaller degree polynomial satisfying the above – and this contradicts the minimality of l. We have thus shown that for all $\alpha \in K$ there is a corresponding irreducible monic polynomial of degree d. But some of these polynomials may be the same – fortunately, we can account for all the repetitions by noting that each polynomial of degree d has at most d roots – hence a polynomial can repeat at most d times. So, by going through all values of α we can construct $(|K|-1)/d$ monic irreducible polynomials. Since $|K| = q^d$, we have shown that there are at least $(q^d-1)/d$ distinct monic irreducible polynomials of degree at most d. ■

3.5 Properties of $x^{q^d} - x$

We state and prove two lemmas about the polynomial $x^{q^d} - x$.

Lemma 9 *Let $f(x)$ be an irreducible polynomial. Then $f(x) | x^{q^d} - x$ if and only if* $\deg(f) | d$.

Proof Consider the field K that's the extension of F containing all and only the roots of $x^{q^d} - x$. Since $f(x) | x^{q^d} - x$ there must be an element $\alpha \in K$ such that $f(\alpha) = 0$. Now let's consider the field $F(\alpha) = \{\sum_{i=0}^{\deg(f)-1} \lambda_i \alpha^i \mid \lambda_i \in F\}$. Now, $K \supseteq F(\alpha) \supseteq F$ which implies that $[K : F(\alpha)][F(\alpha) : F] = [K : F]$. Now, $F(\alpha)$ has $q^{\deg(f)}$ elements – hence $[F(\alpha) : F] = \deg(f)$; $[K : F] = d$ therefore $\deg(f) | d$. ■

The following lemma and its consequence are from Lidl and Niedereitter's book on Finite fields.

Lemma 10 *$x^{q^d} - x =$ the product of all monic, irreducible polynomials f where* $\deg(f) | d$.

Proof This follows immediately from the fact that $x^{q^d} - x$ has no repeated factors and from the previous lemma. ■

The lemma above leads to a tight estimate on the number of irreducible polynomials of degree d. Let $N(i)$ denote the number of monic irreducible polynomials of degree i. Then, by considering the degrees of the LHS and the RHS above, we have

$$q^d = \sum_{i|d} i N(i).$$

By Moebius inversion, the above equation implies:

$$N(d) = (1/d) q^d \sum_{i|d} \mu(d/i),$$

where

$$\mu(k) = \begin{cases} 1 & \text{if } k = 1 \\ (-1)^i & \text{if } k \text{ is a product of } i \text{ distinct primes.} \\ 0 & \text{if } p^2 | k \text{ for some prime } p. \end{cases}$$

Using the crude estimates: $\mu(1) = 1$ and $\mu(k) \geq -1$ we get $N(d) \geq \frac{1}{d}\left(q^d - \frac{q^d - q}{q-1}\right)$. In particular, $N(d)$ is at least 1 for every d.