6.885 Algebra and Computation September 28, 2005

Lecture 6

Lecturer: Madhu Sudan *Scribe: Arnab Bhattacharyya*

In the last lecture, we saw an algorithm to find roots of a polynomial in a finite field. In particular, we noticed that if a polynomial $f(x) \in F_q[x]$ has any roots, then $\gcd(f(x), x^q - x)$ is not 1. This is true because $\prod_{\alpha \in F_q}(x - \alpha) = x^q - x$ and, so, a nontrivial common divisor between $x^q - x$ and $f(x)$ indicates that $f(x)$ has linear factors. We can use this gcd test to determine irreducibility of a cubic polynomial, since a cubic factors iff one of its factors is linear. But, in general, if $f(x) \in F_q[x]$ is a monic, degree d polynomial, how do we determine if it is irreducible? We will answer this question in today's lecture.

1 Some Properties of Finite Fields

1.1 Order of a finite field

Let F be a finite field. Then, we claim that $|F| = p^t$ for some prime p and some positive integer t. Let us see why this is true.

First of all, define the characteristic of a ring R to be the smallest integer n such that for all $\alpha \in R$, $n \cdot \alpha = 0$ (if such an n exists). For a field F, the characteristic is equivalently[1] the smallest integer n such that $n \cdot 1 = 0$. Now suppose n is not prime. Let $n = pq$ with $p \leq q < n$. Then, $p \cdot 1 \neq 0$ and $q \cdot 1 \neq 0$ but $(p \cdot 1)(q \cdot 1) = (pq) \cdot 1 = 0$, contradicting the fact that F is an integral domain. So, the characteristic of F is always a prime.

From the above, it easily follows that $\mathbb{Z}_p \subseteq F$; in other words, F is an extension field of $\mathbb{Z}_p$. We have the following fact about extensions of finite fields:

Claim 1 *Let K and L be finite fields with $K \subseteq L$. Then, L can be viewed as a finite-dimensional vector space over K.*

Proof Idea Addition in the K-vector space is the addition law in L and scalar multiplication of an element α in L by an element c of K is defined to be the product $c\alpha$ as multiplied in L. Since L is finite, L must be finite dimensional over K. ■

So, there must exist a finite set of bases elements $b_1, \ldots, b_t$ in L such that $L = \{\sum_i \alpha_i b_i | \alpha_i \in K\}$ and, furthermore, if there exists $\alpha_1, \ldots, \alpha_t$ such that $\sum_i \alpha_i b_i = 0$, then $\alpha_1 = \cdots = \alpha_t = 0$. Thus, if F is a t-dimensional vector space over $\mathbb{Z}_p$, $|F| = p^t$ because there are p choices for each of the t α_i's. This is what we wanted to show.

1.2 Extension fields and subfields

The following constrains the number of subfields of a field:

Claim 2 *Let K, F, L be fields such that $K \subseteq F \subseteq L$, then the dimension of F over K must divide the dimension of L over K.*

Proof Idea Suppose $\{\alpha_i\}$ is a set of bases elements of F over K and $\{\beta_j\}$ a set of bases elements of L over F. Then, $\{\alpha_i \beta_j\}$ is a set of bases elements of L over K. ■

Let L be a t-dimensional vector space over K. Then, if $|K| = q$, $|L| = q^t$. The following claims that there is no other subfield of L isomorphic to K.

Claim 3 *If $K \subseteq L$, then*

[1] Let m be the smallest integer such that $m \cdot 1 = 0$. Then, since $n \cdot 1 = 0$, $n \geq m$. Conversely, for any $\alpha \in F$, $m \cdot \alpha = (m \cdot 1)\alpha = 0$ and, so, $m \geq n$. Therefore, $n = m$.

- *there exists a unique isomorph of K in L*
- *given $\alpha \in L$, one can tell if α is in K or not*

Proof Idea Every $\alpha \in K$ satisfies $\alpha^q = \alpha$, and at most q elements in L satisfy this equation. So, there cannot be another subfield of L of order q, and $\alpha \in K$ if and only if $\alpha^q = \alpha$. ■

The next question that we want to address is whether there are efficient ways to go from the larger field, L, to the smaller field, K. In general, we don't know any good way of enumerating all the elements of K other than by checking each element of L to see if it is a fixed point of the map $x \to x^q$. But there are efficient maps from L to K:

1. **Trace**: Let $Tr_K : L \to L$ be the map defined by

$$Tr_K(x) = x + x^q + x^{q^2} + \cdots + x^{q^{t-1}}$$

Claim 4 *Then,*

- *For all $\alpha \in L$, $Tr_K(\alpha) \in K$*
- *For all $a, b \in K$ and $\alpha, \beta \in L$, $Tr_K(a\alpha + b\beta) = a \cdot Tr_K(\alpha) + b \cdot Tr_K(\beta)$*

Proof Let us prove the second part first. First of all, note that for any x and y in L and for any positive integer i, $(x+y)^{q^i} = x^{q^i} + y^{q^i}$; this fact is used very frequently in finite field calculations. So,

$$\begin{aligned} Tr_K(a\alpha + b\beta) &= \sum_{i=0}^{t-1} (a\alpha + b\beta)^{q^i} \\ &= \sum_{i=0}^{t-1} a^{q^i}\alpha^{q^i} + \sum_{i=0}^{t-1} b^{q^i}\beta^{q^i} \\ &= \sum_{i=0}^{t-1} a\alpha^{q^i} + \sum_{i=0}^{t-1} b\beta^{q^i} \\ &= a \cdot Tr_K(\alpha) + b \cdot Tr_K(\beta) \end{aligned}$$

To see that $Tr_K(\alpha) \in K$ for all $\alpha \in L$, note that

$$\begin{aligned} (Tr_K(\alpha))^q &= \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^t} \\ &= \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{t-1}} + \alpha \\ &= Tr_K(\alpha) \end{aligned}$$

■

2. **Norm:** Let $N_K : L \to L$ be the map defined by

$$N_K(x) = x^{1+q+q^2+\cdots+q^{t-1}}$$

Claim 5 *Then,*

- *For all $x, y \in L$, $N_K(x \cdot y) = N_K(x) \cdot N_K(y)$*
- *$N_K(0) = 0$ and N_K maps L^* to K^**

Proof Idea Similar to above proof of the properties of trace. ■

2 Representing Extension Fields

Suppose we have a way to represent elements of field K, and we would to like to represent elements of an extension field $L \supseteq K$. We will describe three representations, the last of which, using irreducible polynomials, is the most standard one.

2.1 (Partial) Representation 1

We argued above that L, a field of order q^t, is isomorphic to a t-dimensional (additive) vector space over K, a field of order q. So, one way to represent an element $\alpha \in L$ is as a vector $V_\alpha \in K^t$. This is suitable for addition because $V_{\alpha+\beta} = V_\alpha + V_\beta$, but it is not suitable for multiplication.

2.2 Representation 2

Let us modify the above representation in order to encode the field multiplication table. For each $\alpha \in L$, consider the linear map $A_\alpha : K^t \to K^t$ defined to be $A_\alpha(V_\beta) = V_{\alpha\beta}$. Also, note that $A_\alpha(V_\beta + V_\gamma) = A_\alpha V_\beta + A_\alpha V_\gamma$, satisfying the distributive law. Each A_α can be encoded by a t-by-t matrix over K. Hence, this representation is suitable for doing addition and multiplication over L. However, it is often the case that we cannot afford the $O(t^2)$ elements required to represent each element in L.

2.3 Representation 3

We will show that for all positive integers t, there exists a polynomial $g(x) \in K[x]$ of degree t that is monic and irreducible. Furthermore, $L \cong K[x]/(g(x))$. Thus, an element of L can be represented as a polynomial in $K[x]$ of degree less than t.

Claim 6 *Given a field K of order q and any positive integer t, there exists a field $L \supseteq K$ of order q^t.*

Proof Idea Consider the polynomial $f(x) = x^{q^t} - x$. Let F be the extension field of K over which this polynomial splits completely into linear factors. We can always find F by repeatedly adjoining roots to K. Now, we will show that $L = \{\alpha \in F | \alpha^{q^t} - \alpha = 0\}$ is the desired field of order q^t.

First of all, since $f'(x) = -1$ and, so, $\gcd(f, f') = 1$, $f(x)$ has no repeated roots. Combining this with the fact that $f(x)$ has at most q^t roots leads us to $|L| = q^t$.

Next, we need to see that L is a field. This is pretty straightforward. If $\alpha, \beta \in L$, then clearly $\alpha\beta$ and α^{-1} are in L; also, $\alpha + \beta \in L$ because $(\alpha+\beta)^{q^t} = \alpha^{q^t} + \beta^{q^t}$ and $-\alpha \in L$ because $(-1)^{q^t} = -1$ for odd q and $-1 = 1$ for a field of characteristic 2. ■

It is also true that any two fields of the same order are isomorphic, although we shall not prove this claim here. (Therefore, in many places, we will say "a field" where "the field" is also true.)

Next, we define the concept of a minimal polynomial $g_\alpha(x) \in K[x]$ for an $\alpha \in L$. If $\alpha \in K$, then its minimal polynomial is $g_\alpha(x) = x - \alpha$. Otherwise, if $\alpha \in L - K$, consider the smallest set $\{1, \alpha, \alpha^2, \ldots, \alpha^d\}$ such that there exists $c_0, \ldots, c_d \in K$ with $\sum_{i=0}^{d} c_i \alpha^i = 0$ and $c_d = 1$. Then call $g_\alpha(x) = \sum_{i=0}^{d} c_i x^i \in K[x]$ the minimal polynomial for α. Note that $d \leq t$ because there can be at most t linearly independent elements in L regarded as a K-vector space.

Claim 7 *For any $\alpha \in L$, $g_\alpha(x)$ is an irreducible polynomial over K.*

Proof Suppose $g_\alpha(x)$ is not irreducible; that is, $g_\alpha(x) = h_1(x)h_2(x)$ for some $h_1, h_2 \in K[x]$ and $\deg(h_1) \leq \deg(h_2) < \deg(g_\alpha)$. Then, since $g_\alpha(\alpha) = 0$ and $K[x]$ is an integral domain, $h_1(\alpha) = 0$ or $h_2(\alpha) = 0$. But this is a contradiction to the minimality of $d = \deg(g_\alpha)$. ■

Next, we show that there do exist irreducible polynomials of degree d for all positive integers $d \leq t$.

Claim 8 *For any field K, there exist at least $\frac{q^d-1}{d} - q^{d/2}$ irreducible polynomials in $K[x]$ of degree d.*

Proof Consider a field L of order q^d as guaranteed by Claim 6. Then, we can construct minimal polynomials from each nonzero $\alpha \in L$. Some of these polynomials may be the same, but since a polynomial of degree d has at most d roots, each polynomial can repeat at most d times. Hence there are at least $\frac{q^d-1}{d}$ irreducible polynomials of degree less than or equal to d. Next, note that the degree of each irreducible polynomial must divide d. This is so, because if an irreducible polynomial g has degree r, then $K[x]/(g(x))$ has dimension r over K and hence, by Claim 2, r must divide d, the dimension of L over K. Therefore, the next highest degree of an irreducible polynomial after d is $d/2$ and there are a total of $q^{d/2}$ polynomials of degree $d/2$. So, the number of irreducible polynomials of degree strictly d is at least $\frac{q^d-1}{d} - q^{d/2}$. ■

The above claim should cover most combinations of q and d; for those not covered, the requisite irreducibles are listed in some book! Note that this claim is analogous to the version of the prime-number theorem which states that the probability that an integer of n or less bits is prime is approximately $1/n$.

So, we have shown that given an extension field L of dimension t over K, it is always possible to find an irreducible polynomial $g(x) \in K[x]$ of degree t. Also, it is clear that $K[x]/(g(x))$ is a field of order q^t since $g(x)$ is irreducible. By the isomorphism theorem mentioned above, $L \cong K[x]/(g(x))$. Thus, we can always represent a field element of L as a polynomial in $K[x]$ modulo an irreducible $g(x)$.

3 Testing Irreducibility

Given a $g(x) \in K[x]$ that is monic and of degree d, how do we efficiently decide if it is irreducible? We have now acquired the tools necessary to give the algorithm.

Claim 9 *If $g(x) \in K[x]$ is irreducible of degree d, then $g(x) \mid x^{q^d} - x$.*

Proof Let $L = K[x]/(g(x))$. (Note this is one of those places where introducing an extension field is useful even if there was no mention of one in the original problem.) Then, if $\alpha \in L$, $\alpha^{|L|} = \alpha^{q^d} = \alpha$. Representing α as a polynomial $p(x)$ in $K[x]/(g(x))$, we have that $p(x)^{q^d} = p(x) \pmod{g(x)}$. Letting $p(x) = x$, we have what we wanted. ■

Claim 10 *If $g(x)$ is irreducible of degree d, then for all $d' < d$, $g(x) \nmid x^{q^{d'}} - x$.*

Proof Suppose $g(x) \mid x^{q^{d'}} - x$ for some $d' < d$. Then, consider a splitting field L of $x^{q^{d'}} - x$; $|L| = q^{d'}$. So, g must have a root α in L. Let h_α be the minimal polynomial in $K[x]$ for $\alpha \in L$. Note that $\deg(h_\alpha) \leq d' < d = \deg(g)$; so, $h_\alpha \neq g$. Now, because $x - \alpha$ divides both h_α and g, $\gcd(h_\alpha, g)$ is nontrivial. Also, the gcd is a polynomial in $K[x]$, a contradiction of the fact that g and h_α are irreducible polynomials. ■

Thus, we get the following algorithm for testing irreducibility:

- $d' \leftarrow d - 1$
- Decrement d' until $d' = 1$
  - If $\gcd(g(x), x^{q^{d'}} - x) \neq 1$, output `reducible`
- If $g(x) \mid (x^{q^d} - x)$, output `irreducible`. Else, output `reducible`.

If $g(x)$ is irreducible, then by the above two claims, the algorithms outputs `irreducible`. If $g(x)$ is reducible, say $g(x) = h_0(x)h_1(x)$ where h_0 is irreducible of degree $d_0 < d$. Then, by Claim 9, $h_0(x)$ divides $x^{q^{d_0}} - x$ and, so, $\gcd(g(x), x^{q^{d_0}} - x) \neq 1$ and the algorithm returns `reducible`.