Algebra and Computation Course Instructor: V. Arvind

Lecture 11: Some field theory and irreducibility tests

Lecturer: V. Arvind *Scribe: Kazim Bhojani and Shreevatsa R*

1 Crash course in Field theory

Definition, size is prime power, the generating function counting, cyclic,

$$X^{q^n} - X = \prod_{\substack{\deg f | n \\ f \text{ monic and irreducible in } \mathbb{F}_q[X]}} f(X) \tag{1}$$

the equality with the product of irreducible polynomials, uniqueness

2 Algorithms

We now have enough understanding of fields to look at various problems.

In general, we will be given as input a field $\mathbb{F}_q$, where $q = p^m$ for some prime number p. It is unreasonable to expect to be given $\mathbb{F}_q$ as a list of elements and addition/multiplication tables. As $\mathbb{F}_q = \mathbb{F}_p[X]/(h(X))$ for some irreducible polynomial $h(X)$ of degree m, it can be specified by p and the coefficients of $h(X)$, and that is what we are given. (This contributes $m \log p = \log q$ to the input size, and a particular element of $\mathbb{F}_q$ can be written down using $\log q$ bits).

2.1 Testing Irreducibility

Given a polynomial $f(X)$ of degree n over $\mathbb{F}_q$, we want to test whether it is irreducible.

The input needs to specify the coefficients of $f(X)$, each of which is an element of $\mathbb{F}_q$, so the input size is $(\deg f)(\log q)$.

We observe that by **??**, if $f(X)$ is irreducible, it must divide $X^{q^n} - X$, i.e., $\gcd(f(X), X^{q^n} - X) = f(X)$. Conversely, if $f(X)$ is not irreducible, there exists some d less than n such that $\gcd(f(X), X^{q^d} - X) \neq 1$.

Thus we have reduced testing irreducibility to finding the gcd of two polynomials, which is simply Euclid's algorithm. Note here that although the polynomials $X^{q^d} - X$ are of exponentially large degree, we only need them

modulo $f(X)$, and we can easily compute X^r modulo $f(X)$ for exponential r in polynomial time by using the repeating squaring algorithm for powering.

2.2 Factorisation: Cantor–Zassenhaus algorithm

The next thing we would like to do is to actually factorise $f(X)$ into its irreducible factors. In this subsection, we describe an algorithm due to Cantor and Zassenhaus which is randomised and is in Las Vegas polytime.

Firstly, note that any repeated factors of f are factors of $\gcd(f, f')$ as well. In fact, if $f = g_1^{l_1} g_2^{l_2} \dots g_r^{l_r}$, then $\frac{f}{\gcd(f,f')} = g_1 g_2 \dots g_r$, and once we have the factorisation of the latter, we can easily find each l_i as the highest power of g_i that is present in f. So we can assume f is square-free.

Further, we can use the gcd idea (**??**) to separate out the irreducible factors of degree d, for every d. That is, let

$$f_1 = \gcd(f, X^q - X) \qquad f \leftarrow \frac{f}{f_1}$$

$$f_2 = \gcd(f, f, X^{q^2} - X) \qquad f \leftarrow \frac{f}{f_2}$$

and so on, then $f_1(X)$ is the product of all the linear factors, $f_2(X)$ is the product of all the quadratic factors, and in general, $f_d(X)$ is the product of all the irreducible factors of $f(X)$ of degree d. We can deal with each the f_ds separately. So we can assume $f = g_1 g_2 \dots g_r$ where all the g_i are irreducible and of (known) degree d.

By the Chinese Remainder Theorem,

$$\begin{aligned}\frac{\mathbb{F}_q[X]}{(f(X))} &\cong \frac{\mathbb{F}_q[X]}{(g_1(X))} \times \dots \times \frac{\mathbb{F}_q[X]}{(g_r(X))} \\ &\cong \mathbb{F}_{q^d} \times \dots \times F_{q^d}\end{aligned}$$

(We proved the Chinese Remainder Theorem here)

Of the nonzero elements in $\mathbb{F}_q[X]/(f(X))$, the units (those with gcd 1 with $f(X)$) are large in number — there are $(q^d - 1)^r$ of them, out of the $q^n = q^{dr}$ total. What we would like to get, for factorisation, are the zero divisors (those with nontrivial gcd with $f(X)$).

2.2.1 If q is odd

For each $x \in \mathbb{F}_{q^d}^*$, $x^{q^d-1} = 1$, and $x^{\frac{q^d-1}{2}}$ is $+1$ or -1 with probability $\frac{1}{2}$ each. This means that $a(X) \mapsto a(X)^{\frac{q^d-1}{2}} - 1$ takes $a(X)$ to $(\pm 1 - 1, \pm 1 -$

$1, \ldots, \pm 1 - 1$), which is zero only when every "co-ordinate" is 0 and a unit only when each of them is -2, each of which happens with probability $\frac{1}{2^r}$. Thus, with probability $1 - \frac{2}{2^r}$, we get a zero divisor, whose gcd with $f(X)$ gives us a factor. We can now remove this factor, test for irreducibility, and recurse.

2.2.2 If q is even

When q is even (the characteristic is 2), the above does not work as 1 and -1 are the same. q is a power of 2, say $q = 2^k$.

The mth trace polynomial is defined as

$$T_m(X) = X + X^2 + X^{2^2} + X^{2^3} + \cdots + X^{2^{m-1}}$$

Consider

$$\begin{aligned} T_m(X)(T_m(X)+1) &= T_m(X)^2 + T_m(X) \\ &= T_m(X^2) + T_m(X) && \text{characteristic 2} \\ &= x^{2^m} + x && \text{everything else occurs twice} \end{aligned}$$

For any m, in $\mathbb{F}_{2^m}$, $T_m(T_m + 1)$ splits as $\prod_{\alpha \in \mathbb{F}_{2^m}} x - \alpha$. For a random element $\alpha \in \mathbb{F}_{2^m}$, $\Pr[T_m(\alpha) = 0] = \Pr[T_m(\alpha) = 1] = \frac{1}{2}$. We have

$$\frac{\mathbb{F}_q[X]}{(f(X))} \cong \mathbb{F}_{2^{kd}} \times \cdots \times \mathbb{F}_{2^{kd}}$$

so for $m = kd$, $T_m(a(X))$ is a zero divisor with probability $1 - \frac{2}{2^r}$. As before, we can get a factor, remove it, and recurse.

2.3 Factorisation: Berlekamp's algorithm

The Cantor–Zassenhaus algorithm is randomised. Berlekamp's algorithm is a deterministic algorithm, which runs in polynomial time when the q is small.

As before, we can remove repeated factors of f, so we can assume that $f = g_1 g_2 \ldots g_r$ where all the g_is are distinct irreducible factors.

Now consider the map

$$\phi : \frac{\mathbb{F}_q[X]}{(f(X))} \to \frac{\mathbb{F}_q[X]}{(f(X))}$$

defined as $a \mapsto a^q - a$. This is a linear map (check).

Let $\mathcal{B} = \ker(\phi) = \left\{ a \in \frac{\mathbb{F}_q[X]}{(f(X))} \ : \ a^q = a \right\}$.

Let $\psi : \frac{\mathbb{F}_q[X]}{f} \to \frac{\mathbb{F}_q[X]}{g_1} \times \cdots \times \frac{\mathbb{F}_q[X]}{g_r}$ be the isomorphism given by the Chinese Remainder Theorem. $\psi((B)) = \mathbb{F}_q \times \cdots \times \mathbb{F}_q$.

We want to find (B) – that is, find a basis for it. This is easy; we can find out for each X^j its image $X^{qj} - X^j \bmod f$, and hence write down the matrix for the linear map ϕ.

Note that the elements of (B) are precisely the zero divisors. So we can sample from (B), and use the zero divisors to get factors of f, remove them and recurse, as before.