CS681 **Computational Number Theory**

Lecture 12: Berlekamp's Algorithm

Instructor: Piyush P Kurur *Scribe: Ramprasad Saptharishi*

Overview

Last class we say a randomized algorithm for factoring univariate polynomials over a finite field. This class we shall look at another algorithm for factoring. This was given by Berlekamp.

1 Berlekamp's Algorithm

We are given a polynomial $f(X) \in \mathbb{F}_p[X]$. As in all factoring algorithms, the first thing to do is make f square free. Once we have done this, the polynomial is of the form

$$f = f_1 f_2 \cdots f_m$$

where each f_i is a distinct irreducible factor of f. Then, chinese remaindering tells us that

$$R = \mathbb{F}_p[X]/(f) = (\mathbb{F}_p[X]/(f_1)) \times (\mathbb{F}_p[X]/(f_2)) \times \cdots \times (\mathbb{F}_p[X]/(f_m))$$

Let the degree of f_i be d_i and the degree of f be n.

1.1 The Frobenius Map

Here enters the frobenius map again. Consider the following function from R to itself.

$$\begin{array}{rcl} T : R & \longrightarrow & R \\ a & \mapsto & a^p \end{array}$$

The first thing to note here is that all elements of $\mathbb{F}_p$ are fixed in this map because we know that elements $\mathbb{F}_p$ satisfy $X^p - X = 0$. And further, we also saw the special case of binomial theorem that said $(X+Y)^p = X^p + Y^p$.

To understand this map T better, let us understand R. We have defined $R = \mathbb{F}_p[X]/(f)$ which is basically polynomials over $\mathbb{F}_p$ modulo f. And clearly, every element of R has degree atmost $n-1$ and therefore a polynomial of the form $a_0 + a_1X + \cdots a_{n-1}X^{n-1}$ can be thought of as the vector $(a_0, a_1, \cdots, a_{n-1})$. Thus, the ring R is a vector space of dimension n over $\mathbb{F}_p$.

Now, notice that the map T described above is $\mathbb{F}_p$-linear. By this, we mean that for all $\alpha, \beta \in \mathbb{F}_p$ and $u, v \in R$, we have $T(\alpha u + \beta v) = \alpha T(u) + \beta T(v)$. If we think of these elements of $\mathbb{F}_p$ as scalars, they can be 'pulled out of' T.

Therefore, it's enough to know the image of each X^i by the map.

$$\begin{aligned} p(X) &= a_0 + a_1X + \cdots + a_{n-1}X^{n-1} \\ T(p(X)) &= a_0 + a_1T(X) + \cdots + a_{n-1}T(X^{n-1}) \end{aligned}$$

1.2 The Berlekamp Sub-algebra

Now let B be the map $T - I$ where I is the identity map (maps everything to itself). Then B sends any element $a \in R$ to $a^p - a$. Now define $\mathcal{B} = \ker(B) = \ker(T - I)$. It is easy to check that the kernel of any linear map from one vector space into another (in this case R to R) forms a subspace of the vector space. Hence $\mathcal{B}$ is a subspace of the vector space R.

This space $\mathcal{B}$ is called the Berlekamp sub-algebra.

What does this space look like? Let a be any element in $\mathcal{B}$ and therefore is an element of R. Let the chinese remainder theorem map this to the tuple $(a_1, a_2, \cdots, a_m)$. And therefore $a^p - a = (a_1^p - a_1, \cdots, a_m^p - a_m)$. And since $a \in \mathcal{B}$, each of the $a_i^p - a_i$ must be 0. Now, $a_i^p - a_i$ is an element of $\mathbb{F}_p[X]/(g_i) \cong \mathbb{F}_{p^{d_i}}$ and therefore $a_i^p - a_i = 0$ can happen only if $a_i \in \mathbb{F}_p$.[1]

And therefore, each element of the tuple will infact be an element of $\mathbb{F}_p$ and therefore

$$\mathcal{B} \cong \mathbb{F}_p \times \cdots \times \mathbb{F}_p$$

And since $\mathcal{B}$ is a product of m copies of $\mathbb{F}_p$, $\mathcal{B}$ is an m dimensional subspace of R over $\mathbb{F}_p$.

[1] the elements of $\mathbb{F}_{p^d}$ that satisfy $X^p - X = 0$ are precisely those elements of $\mathbb{F}_p$

1.3 Finding a Basis

A basis for R is obvious, $\left\{1, X, X^2, \cdots, X^{n-1}\right\}$ but how do we find a basis for $\mathcal{B}$? Let us say T acts on R as

$$T(X^i) = \sum_{j=0}^{n-1} \alpha_{ji} X^j$$

then we can think of T as a the matrix $(\alpha_{ji})_{i,j}$. Thus, thinking of polynomials in R as a tuple of coefficients described above, then the action of T is just left multiplication by this matrix.

Thus, the matrix for B would be $\hat{B} = (\alpha_{ji})_{i,j} - I$. Hence the kernel of this map is just asking for all vectors v such that $\hat{B}v = 0$. And therefore, a basis for $\mathcal{B}$ can be obtained by gaussian elimination of $\hat{B}$.

Once we have a basis $\{b_1, b_2, \cdots, b_m\}$, we can pick a random element of $\mathcal{B}$ by just picking m random elements a_m from $\mathbb{F}_p$ and $\sum a_i b_i$ would be our random element from $\mathcal{B}$.

Any element a in $\mathcal{B}$ gets mapped to $\mathbb{F}_p \times \cdots \times \mathbb{F}_p$ by the Chinese remainder theorem. And therefore, we can use the Cantor-Zassenhaus idea there: $a^{\frac{p-1}{2}}$ corresponds to a vector of just 1s and -1s.

So here is the final algorithm.

Algorithm 1 BERLEKAMP FACTORIZATION

Input: A polynomial $f \in \mathbb{F}_p[X]$ of degree n

1. Make f square-free.
2. Let R be the ring $\mathbb{F}_p[X]/(f)$, considered as a n dimensional vector space over $\mathbb{F}_p$.
3. Construct the matrix of transformation $\hat{B}$ corresponding to the map $a \mapsto a^p - a$.
4. Use gaussian elimination and find a basis $\{b_1, b_2, \cdots, b_m\}$ for the berlekamp subalgebra $\mathcal{B}$.
5. Pick $\{a_1, \cdots, a_{m-1}\} \in_R \mathbb{F}_p$ and let $b = \sum a_i b_i$.
6. **if** $gcd(b^{\frac{p-1}{2}} + 1, f)$ is non-trivial **then**
7.   **return** $gcd(b^{\frac{p-1}{2}} + 1, f)$ {Happens with probability atleast $1 - 2^{m-1}$}
8. **end if**
9. Repeat from step 5.
