Algebra and Computation Course Instructor: V. Arvind

Lecture 13: More on Univariate Factorization over $\mathbb{F}_q$

Lecturer: V. Arvind *Scribe: Ramprasad Saptharishi*

1 Overview

(the initial part of this lecture has been appended to lecture 11 *for continuity.)*

In the earlier lectures we saw univariate polynomial factoring when the characteristic of the field is small. Before we get into bivariate polynomial factoring (which has all the essentials needed for general multivariate factoring), we shall look at some problems closely related to the things we have seen.

2 Factoring $\leq_P$ Root-Finding

In the earlier lectures, we saw factorization of univariate polynomials over a finite field of small characteristic. What about the case when p is large, polynomially many bits long? In this section, we shall show that the problem can be reduced that of finding a root of a polynomial over the prime field $\mathbb{F}_p$.

The polynomial has an additional promise that it splits over $\mathbb{F}_p$ (all its roots are contained in $\mathbb{F}_p$). We will show that finding a non-trivial factor of a polynomial reduces to finding a root of such a polynomial over the prime field. The rest of the section will be a proof of this theorem.

Theorem 1. *Given $f \in \mathbb{F}_q[x], q = p^m$, we can, in polynomial time, reduce it to the problem of finding a root of a polynomial $g \in \mathbb{F}_p[x]$ with the promise that all its roots are in $\mathbb{F}_p$.*

The following simple proposition is the core of the reduction.

Proposition 2. *For any $f, g \in F[x]$, polynomials over some field, $\gcd(f,g) \neq 1$ if and only if there exists $s, t \in F[x]$ such that $\deg s < \deg f, \deg t < \deg g$ and $fs + gt = 0$.*

Proof. Obvious! (take $s = f/\gcd(f,g)$ and $t = -g/\gcd(f,g)$) □

$P_m = \{s \in F[x] \ : \ \deg s < m\}$ and $P_n = \{t \in F[x] \ : \ \deg t < n\}$, the set of all possible s and t for the Let the $\deg f = n$ and $\deg g = m$. Look at the following sets proposition; they form a vector space over F. Once we fix f and g, we have the following linear map:

$$\begin{array}{rcl} \theta : P_m \times P_n & \longrightarrow & P_{n+m} \\ (s,t) & \mapsto & sf + gt \end{array}$$

The proposition tells us that the above linear map is invertible if and only if $\gcd(f,g) = 1$. Let us fix a basis for the two spaces so that we can find the matrix for the linear map.

The natural basis for $P_m \times P_n$ is

$$\big\{(X^{m-1},0),(X^{m-2},0),\cdots,(1,0)\big\} \cup \big\{(0,X^{n-1}),(0,X^{n-2}),\cdots,(0,1)\big\}$$

and that for P_{m+n} as just

$$\big\{X^{m+n-1},X^{m+n-2},\cdots,1\big\}$$

Suppose $f = f_0 + f_1x + f_2x^2 + \cdots f_nx^n$ and $g = g_0 + g_1x + \cdots g_mx^m$, it is easy to see that the matrix for θ is the following:

$$\mathcal{S} = \begin{bmatrix} f_n & 0 & \cdots & 0 & g_m & \cdots & 0 \\ f_{n-1} & f_n & \cdots & & g_{m-1} & \ddots & \vdots \\ f_{n-2} & f_{n-1} & \ddots & \vdots & \vdots & \vdots & g_m \\ \vdots & \vdots & \cdots & f_n & \vdots & \ddots & \vdots \\ \vdots & \vdots & \cdots & \vdots & g_0 & \vdots & \vdots \\ f_0 & f_1 & \cdots & \vdots & 0 & \vdots & \vdots \\ 0 & f_0 & \cdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & f_0 & 0 & \cdots & g_0 \end{bmatrix}_{(m+n)\times(m+n)}$$

The matrix is called the *Sylvester Matrix*, named after the mathematician. The determinant of the matrix is called the resultant of f, g (denoted by $Res(f,g)$). The proposition tells us that $Res(f,g) = 0$ if and only if $\gcd(f,g) \neq 1$.

From Berlekamp's algorithm, if $a \in \ker \phi$ (the Berlekamp kernel), then $f = \prod_{\alpha \in \mathbb{F}_p} \gcd(f, a-\alpha)$. We want to convert this to a polynomial with roots whenever $\gcd(f, a-\alpha) \neq 1$. The idea is to look at α as an indeterminate. Now $Res_x(f, a-Y)$ will now be a polynomial in Y with a root α whenever $\gcd(f, a-\alpha) \neq 1$.

The roots we are looking for are certainly in $\mathbb{F}_p$, but we need the extra property that it infact splits in $\mathbb{F}_p$. But that can be done easily, all that we need to do is take $P(Y) = \gcd(Y^p - Y, Res_x(f, a-Y))$ since the polynomial $Y^p - Y$ as $\prod_{\alpha \in \mathbb{F}_p}(Y - \alpha)$.

Clearly, whatever we have done is a polynomial time computation (determinant by just gaussian elimination, gcd trick as done in the earlier lectures, finding an element in berlekamp kernel by gaussian elimination, etc) and reduces finding a non-trivial factor to finding a root of a special polynomial.

3 How to Share a Secret

This problem arises in the context of secure multiparty computations. Informally, the problem is the following: You have a secret x chosen randomly from a set $\mathcal{S}$ of secrets and it is to be split up into n parts and given to n people (one piece each). You want the pieces to satisfy the following property that the secret can be found if and only if all of them get together.

Formally, $\mathcal{S} \subseteq \mathbb{F}_q$. An element χ chosen from $\mathcal{S}$ uniformly at random. There are n people $(n < q)$, and the problem is to assign each of them pieces such that

- For any proper subset of shares, no information about χ is lost.
- If all of them are together, χ can be found.

The following scheme, Shamir's Secret Sharing Scheme, is a beautiful application of the chinese remaindering theorem.

Choose a polynomial $a(x) = a_0 + a_1 x + \cdots a_{n-1}x^{n-1}$ such that $a_0 = \chi$ and every other a_i is chosen at random from $\mathbb{F}_q$. Pick a polynomial $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ where the α_is are distinct non-zero elements of $\mathbb{F}_q$. By the chinese remaindering theorem, we the isomorphism

$$\psi : \frac{\mathbb{F}_q[x]}{(f(x))} \longrightarrow \frac{\mathbb{F}_q[x]}{(x-\alpha_1)} \times \cdots \frac{\mathbb{F}_q[x]}{(x-\alpha_n)}$$

Thus ψ would send $a(x)$ to the tuple $\langle a(\alpha_1), \cdots, a(\alpha_n)\rangle$. Give the i^{th} person $a(\alpha_i)$.

It is clear that when everyone gets together, they can invert the map ψ and recover a and hence $a(0) = \chi$. We need to argue that no proper subset can be able to recover any information about χ. Without loss of generality, we can assume that the first $n-1$ get together, and say they recover $\langle a_1, \cdots, a_{n-1}, ? \rangle$.

The set of possible polynomials is

$$A = \left\{ a(x) \in \frac{\mathbb{F}_q[x]}{(f)} \ : \ a(x) \mapsto \langle a_1, a_2, \cdots, a_{n-1}, ? \rangle \right\}$$

If $a(x)$ was the actual polynomial, it is clear that $A = a(x) + S$ where

$$S = \left\{ c(x) \in \frac{\mathbb{F}_q[x]}{(f)} \ : \ c(x) \mapsto \langle 0, \cdots, 0, ? \rangle \right\}$$

The set S is precisely the set of polynomials $c = \alpha \prod_{i=1}^{n-1}(x - \alpha_i)$ where α can be any scalar. And it is easy to see that $c(0) = \alpha \prod_{i=1}^{n-1}(-\alpha_i)$ which can again take any possible value in $\mathbb{F}_q$ and hence $a(0) + c(0)$ also takes all possible values in $\mathbb{F}_q$, thus reveals nothing about χ.

4 Towards Bivariate Factoring

We shall next look at bivariate factoring. This does not mean we would look at trivariate factoring next; bivariate factoring contains all the essentials of multivariate factoring.

Before we go into it, we need a crash course in ring theory, definitions and useful theorems at least.

4.1 A Crash Course in Ring Theory

1. Ring: A set R with two operations $\star, +$ such that $(R, +)$ is an abelian group, and $\star$ distributes over $+$. We'll denote $a \star b$ by just ab.

2. Zero divisors: Elements $x \in R$ such that there exists a y such that $xy = 0$.

3. Integral Domains: Commutative rings with a multiplicative identity element called 1 that does not have any non-trivial zero divisors.

4. Irreducible elements in an integral domain: An element x is said to be irreducible if $x = yz$ implies either y or z is a unit.

5. Prime elements in an integral domain: $p \mid ab \implies p \mid a$ or $p \mid b$.

6. The field of fractions of an integral domain: The field of formal fractions, ordered pairs (x, y) interpretted as x/y with addition and multiplication defined naturally.

7. Unique Factorization Domain: An integral domain where factorization into irreducible factors is unique (up to units and rearrangements)

8. Ideal: A subset $I \in R$ such that it is a subgroup under $+$, and satisfies the property that for all $x \in I$ and $r \in R$, $rx \in R$. They are useful for defining homomorphism (kernel of any ring homomorphism is an idea) and quotient rings.

9. Ideal generated by a $a_1, \cdots, a_n$: The smallest ideal containing $a_1, \cdots, a_n$. This is just the set of all elements of the form $\sum_{r_i \in R} r_i a_.$

10. Prime Ideal: An ideal satisfying the property that $xy \in I \implies x \in I$ or $y \in I$.

Some properties:

Fact 1. *prime $\implies$ irreducible*

The converse, however, is not true in general. For example, consider $\mathbb{Q}[X^2, X^3]$. There X^2 is irreducible, but not prime since $X^2 \mid X^3 \cdot X^3$. Nevertheless, they are the same over an UFD.

Fact 2. *If R is a UFD, prime $\Leftrightarrow$ irreducible.*

Fact 3. *In an integral domain, if I is a maximal ideal, the quotient R/I is a field.*

Fact 4. *If I is a prime ideal of R, then R/I is an integral domain.*

Fact 5. *If R is a UFD, then so is $R[x]$.*

The last fact is an important theorem. In particular, since any field is a UFD, $F[X_1, \cdots, X_n]$ is a UFD.

4.2 Towards Bivariate Factorization

The idea is to look at $F[x, y]$ as $F[x][y]$, thinking of $F[x, y]$ as a univariate polynomial extension over $F[x]$ through the variable y. The question is that, can we somehow use the univariate factorization in this context? If we can factorize efficiently in $F[x]$, can we do that in $F[x][y]$ through some bootstrapping?

One possibility is trying to substitute values and factorize, but that would case factors that were initially irreducible to split after substitution. Is there a way by which we can get around this difficulty? We shall explore these problems in the following lecture.