Algebra and Computation Course Instructor: V. Arvind

Lecture 15: Bivariate Factorization: Missing Pieces

Lecturer: V. Arvind *Scribe: Ramprasad Saptharishi*

1 Overview

Last class we did bivariate factorization, but we made some assumptions in the beginning. The hope was that with some preprocessing, the assumptions can be guarenteed. This class we shall see what those preprocessing steps are.

After that, we shall discuass a Hensel Lifting take on Newton's root finding algorithm.

2 The Missing Pieces

The algorithm relies on the assumption that the factorization of f and $f(x,0)$ is square free since we want the pseodo-gcd of factors to be 1. We need to make sure that we can pull out repeated factors in the beginning.

2.1 f is square free

In the univariate case, this was trivial since we just had to take the derivative and do it. Multivariate cases are a little tricky. The first step is to remove the *content* of each variable from the polynomial.

Think of the polynomail f as one over $F[y][x]$, a univariate polynomial with coefficients coming from $F[y]$. The y-content of f is defined as the gcd of the coefficients of the polynomial when considered as one in $F[y][x]$.

The x-content and y-content are clearly factors of f and hence we can factorize them using univariate factorization. Hence we can assume that

$$f = f_1^{e_1} f_2^{e_2} \cdots f_k^{e_k}$$

where each f_i is an irreducible factor with x-content and y-content being 1. Let us look at this as $f = f_1^e h$. Then,

$$\frac{\partial f}{\partial x} = e f_1^{e-1} h \frac{\partial f_1}{\partial x} + f_1^e \frac{\partial h}{\partial x}$$

Suppose both $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ are zero, then the only way this can happen if each power of x and y is a multiple of p. Hence $f(x,y) = g(x^p, y^p)$ and this can be checked easily and it now just amounts to factorizing g.

We can now assume without loss of generality that $\frac{\partial f}{\partial x}$ is non-zero. Now suppose that $\frac{\partial f_1}{\partial x}$ was non-zero, then clearly from the above equation the largest power of f_1 that divides $\frac{\partial f}{\partial x}$ is f^{e-1}.

Let $u = \frac{\partial f}{\partial x}$, $v = \frac{\partial f}{\partial y}$, $u' = f/\gcd(f,u)$ and $v' = f/\gcd(f,v)$, whenever they are non-zero. The bad news is that, since some of the $\frac{\partial f_i}{\partial x}$ could be zero, it misses out the factors that are x^p polynomials. The good news is that, these are the only things that u' and v' would miss.

Hence, factorize u' and v', then divide f by the collection of factors. We are then assured that the remaining factors have to be polynomails of x^p and y^p. We can them make the transformation and recurse.

Thus, we can ensure that f does not have any repeated factors.

2.2 $f(x,0)$ is square free

Though we have $f(x,y)$ to be square free, substituting 0 for y would case certain factors to collapse; $f(x,0)$ could have repeated roots. The trick is to make a small change of variables to ensure that it is square free.

Replace $f(x,y)$ by $f_\beta(x,y) = f(x, y+\beta)$. We need to show that there exists a β such that $f(x,\beta) = f_\beta(x,0)$ is square free.

If $f' = 0$, then reverse the roles of x and y (if both are zero, then it is a polynomial of x^p and y^p). Note that $\gcd(f,f') \neq 1$ if and only if $Res_x(f,f') = 0$. And since the resultant is a polynomial of degree $2d^2$, this can have atmost $2d^2$ roots of F. Hence if $|F| > 2d$, we can just substitute $2d^2+1$ values for y and we would get a polynomial where the residue is non-zero, and thus $f_\beta(x,0)$ would be square free.

Hence, all that's left to do is the case when $|F| \leq 2d^2$. The trick is to go to a larger field and work there. Suppose $F = \mathbb{F}_q$, choose a prime t such that $q^t > 2d^2$ and $t > \deg f$. Replace F by $\mathbb{F}_{q^t}$ (just find an irreducible polynomial of degree t and work in $\mathbb{F}_q$ modulo that polynomial). In this larger field, the irreducible factors could split even further.

$$f = f_1' f_2' \cdots f_{k'}'$$

where bunches of these factors correspond to the original factors. To study these bunches, we need an important map known as the *Frobenius map.*

$$\begin{aligned} \sigma : \mathbb{F}_{q^t} &\longrightarrow \mathbb{F}_{q^t} \\ a &\mapsto a^q \end{aligned}$$

Note that the map fixes every element of $\mathbb{F}_q$ pointwise, and is an automorphism. This can be naturally extended to the ring $\mathbb{F}_q[x, y]$.

And since $f_1 \in \mathbb{F}_q[x, y]$, the frobenius map will fix it. We are interested in finding the bunch of f_i' that correspond to f_1. Suppose $f_1' \mid f_1$, then by the automorphism, $\sigma(f_1') \mid f_1$, $\sigma^2(f_1') \mid f_1$ and so on.

Since $\sigma^t(f_1') = f_1'$, for any r such that $\sigma^r(f_1') = f_1'$ will force r to divide t. Since t is chosen to be a prime, either $r = t$ or $r = 1$. If $r = t$, then each of the t elements of the form $\sigma^i(f_1')$ would be a factor of f_1. But since $t > \deg f$, all of them cannot fit inside f.

Hence $r = 1$, and thus the factorization does not fit further in $\mathbb{F}_{q^t}$. We can now hunt for a β here to make it square free.

3 Hensel Lifting and Newton Rhapson

Suppose we are given a polynomial $f(x) \in \mathbb{Z}[x]$, we want to find a root of f efficiently by successive approximations. We shall do this using Hensel lifting.

Pick a small prime p such that $f(x)$ is square free.

$$\begin{aligned} f(x) &= f_0 + f_1 x + f_2 x^2 + \cdots f_n x^n \\ f(x+h) &= \sum_{i=1}^{n} f_i (x+h)^i \\ &= \sum_{i=1}^{n} f_i (x^i + ihx^i - 1 + \cdots) \\ &= f(x) + hf'(x) + h^2 P(x, h) \end{aligned}$$

Now using Berlekamp's algorithm, find an x such that $f(x) = 0 \pmod p$. Suppose there exists an $\hat{x}$ such that $\hat{x} = x \pmod p$ and $f(\hat{x}) = 0$ then $\hat{x} = x + ap$. And hence

$$\begin{aligned} f(\hat{x}) &= f(x) + apf'(x) + a^2 p^2 P(x, ap) \\ \implies 0 = f(\hat{x}) &= f(x) + apf'(x) \pmod{p^2} \end{aligned}$$

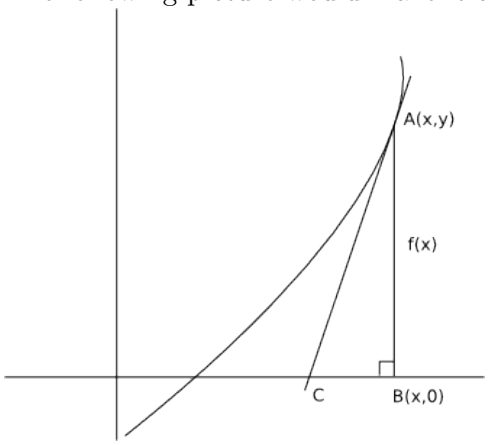
Since $f(x) = 0 \pmod{p}$, it makes sense to talk about $(f(x)/p)$. Thus, if we were to choose $a = (-f(x)/p)\left[f'(x)\right]^{-1}$, the above equation would be satisfied.

$$\begin{aligned} a &= \left(\frac{-f(x)}{p}\right)\left[f'(x)\right]^{-1} \pmod{p} \\ \implies \hat{x} &= x - f(x)\left[f'(x)\right]^{-1} \pmod{p} \end{aligned}$$

Thus, from a factorization modulo p, we have gone up to p^2 with $\hat{x}$ as our next approximation.

Newton-Rhapson also has the similar expression. You are given a function f, you choose a random point x. The next approximation is given by drawing the tangent to the curve f at $(x, f(x))$ and taking the point where this tangent meets the x-axis as its next approximation.

The following picture would make it clear.



If the coordinate of C was $\hat{x}$, our next approximation,

$$\begin{aligned} f'(x) &= \frac{f(x)}{x - \hat{x}} \\ \implies \hat{x} &= x - \frac{f(x)}{f'(x)} \end{aligned}$$

which is exactly what we got in the Hensel Lifting method.

Newton's method however require floating point arithmetic (since division by $f'(x)$ is actual division, unlike inverse modulo p in the hensel lifting case).