CS681 **Computational Number Theory**

Lecture 27 : Bivariate Factoring

Instructor: Piyush P Kurur *Scribe: Ramprasad Saptharishi*

We shall now look at Bivariate Factoring. This is an instance where there are a lot of corner cases that need to be handled but we shall make some preliminary assumptions on the polynomial. We shall soon see how we can ensure those properties as well.

1 Bivariate Factoring

We are given a polynomial $f \in K[X, Y]$ that we would like to factor. Before we go into factorization as such, we first need to figure out how to do the $\gcd$ algorithm over two variables.

1.1 The Euclidian Algorithm for $K[X, Y]$

Lets say we are given two polynomials $f(X, Y)$ and $g(X, Y)$. How do we compute their $\gcd$? Remember that when we had univariate factoring, the euclidian algorithm would divide. But over $K[X, Y]$, how do we do that?

Hence, instead of looking at these polynomials over $K[X, Y]$, we look at them as univariate polynomials rational functions over one variables, namely $K(X)[Y]$. Thus coefficients could now be of the form $p(X)/q(X)$. This then give rise to another problem, can the denominator keep getting larger? That is a serious issue since during the process, we could potentially be doubling the degree at each step

But clearly, the final answer cannot have a really large X-degree; it clearly must be bounded by the X degrees of f and g. So what we do instead is do these computations modulo a number of irreducible polynomials. We just need to make sure that the product of all these irreducible polynomials have degree larger than the X degree of both f and g.

This would then let us compute the $\gcd$ of two bivariate polynomials.

Now we can think of f as an element in $K[X][Y]$, a polynomial in Y each of whose coefficients are polynomials in X. The first things we do is pull out the gcd of all the coefficients. And we also express f as an element of $K[Y][X]$ and repeat the same thing. Then we shall assume that f is

squarefree. This needs justification but we shall do this later. But for the moment let us assume that this can be done and proceed.

Now we have $f(X,Y) \in K[X][Y]$. We shall put $Y = 0$ to get a univariate polynomial in X. Since we have already done factoring of univariate polynomials, we shall factorize $f(X,0)$ into coprime factors $f(X,0) = g_0 h_0$.

Note that this is just saying

$$f = g_0 h_0 \bmod Y$$

since $Y = 0$ is precisely taking $\bmod Y$. And we further have the property, because the factors are coprime[1] that $sg_0 + th_0 = 1 \bmod Y$. Thus we can Hensel Lift this factorization for k steps to get

$$f = g_k h_k \bmod Y^{2^k}$$

We would now argue that after sufficient hensel lifting, we can retrieve a factor of f.

Claim 1. *If f was not irreducible, hen there is an irreducible factor of f, say g such that $g = g_0 l_0 \bmod Y$*

Proof. This is obvious. Suppose f factorizes into irreducible factors as $f_0 f_1 \cdots f_l$. Then clearly,

$$f = f_0 f_1 \cdots f_l \bmod Y$$

And therefore g_0 must divide one of these factors and whatever factor it may be, set that as g. Therefore, $g = g_0 l_0 \bmod Y$ □

Now start with $g = g_0 l_0 \bmod Y$ and lift this to k steps. What we know is that $\deg_X(g) < \deg_X(f)$ and $\deg_Y(g) \leq \deg_Y(f)$. What we have is just $f = g_k h_k \bmod Y^{2^k}$. We shall use this to try and get hold of a factor.

Suppose we look at the following equation to solve:

$$\begin{aligned} \tilde{g} &= g_k \tilde{l} \bmod Y^{2^k} \\ \deg_X(g) &< \deg_X(f) \\ \deg_Y(g) &\leq \deg_Y(f) \end{aligned}$$

Firstly, does this system of equations have a solution? Indeed; we just say that $g = g_0 l_0 \bmod Y$ can be lifted to k steps to give $g = g_k l_k \bmod Y^{2^k}$

[1] we shall get back to this

and clearly g and l_k satisfy the system of equations. Therefore, we are guaranteed that at least one such solution exists if f is not irreducible. Now, how do we compute such a solution?

Notice that we already know g_k and once we have g_k, if we think of the coefficients of $\tilde{g}$ and $\tilde{l}$ as variables, the above is just a system of linear equations. Thus, one could solve that system using gaussian elimination to get some solution $\tilde{g}$. It might very well be possible that $\tilde{g} \neq g$. But from a solution $\tilde{g}$, how do we retrieve a factor?

Look at the two equations $f = g_k h_k \bmod Y^{2^k}$ and $\tilde{g} = g_k \tilde{l} \bmod Y^{2^k}$. And in essence, both f and $\tilde{g}$ share a common factor modulo Y^{2^k}. Therefore, if one were to consider them as polynomials of X with coefficients coming from $K[Y]$, this means that the X-resultant of f and $\tilde{g}$ is zero modulo Y^{2^k}. By the X resultant we mean the resultant, considered as polynomials in $K[Y][X]$.

Therefore

$$\text{Res}_X(f, \tilde{g}) = 0 \bmod Y^{2^k}$$

The resultant would be a polynomial in Y. What is the maximum degree of this polynomial possible? Since we are looking at the determininant, the size of the sylvester matrix is $2m$ where m is the $\deg_X(f)$. And each element of this matrix would be a polynomial in Y of degree at most n where $n = \deg_X(f)$. Therefore, the degree of the resultant polynomial is at most $2mn + 2$. And if 2^k is larger than $2mn + 2$, then

$$\text{Res}_X(f, \tilde{g}) = 0 \bmod Y^{2^k} \implies \text{Res}_X(f, \tilde{g}) = 0$$

and therefore, f and $\tilde{g}$ must infact share a common factor. Use the euclidian algorithm to extract out this factor.

All that is left to do are the corner cases. We shall deal with them in the next class.