6.966 Algebra and Computation	September 30, 1998
Lecture 7	
Lecturer: Madhu Sudan	*Scribe: Daniele Micciancio*

1 Factoring Bivariate Polynomial: Introduction

In this lecture we start the study of bivariate polynomial factorization. We already saw how to factor polynomials in a single variable. Factoring bivariate polynomials is the first step towards our goal of understanding general multivariate factorization. In the following lectures we will see that the steps to go from univariate polynomials to bivariate polynomials are similar (although not exactly the same) to those to go from bivariate to multivariate factorization.

Recall we proved that if R is a unique factorization domain (u.f.d.) then also $R[x]$ is a u.f.d. Similarly, if $R[x]$ is a u.f.d. then also $R[x, y]$ is a u.f.d. By induction, one can show that for any number of variables, if R is a u.f.d., then also $R[x_1, \ldots, x_n]$ is a u.f.d.

One could hope to make the step from R to $R[x]$ algorithmic, i.e., given an algorithm to factor in R, devise a factoring algorithm for $R[x]$. In other words, we want to answer the question: assuming we can factor elements of R, can we factor elements of $R[x]$? We don't know how to answer this for a general R, but we show that when R is a polynomial ring, then factoring in $R[x]$ can be "black-box" reduced to factoring in R. In particular we show that for any u.f.d. R, if we can factor in $R[x]$ (univariate polynomials) than we can factor in $R[x, y]$ (bivariate polynomials).

The idea to go from two variables to one variable is the following. Assume polynomial $f(x, y) \in \mathbb{Z}[x, y]$ factors as

$$f(x, y) = f_1(x, y)f_2(x, y) \cdots, f_n(x, y).$$

Then, the univariate polynomials $f(\cdot, 0)$, $f(\cdot, 1), \ldots$ factor as

$$f(x, 0) = f_1(x, 0)f_2(x, 0) \cdots, f_n(x, 0).$$

$$f(x, 1) = f_1(x, 1)f_2(x, 1) \cdots, f_n(x, 1).$$

$$f(x, 2) = f_1(x, 2)f_2(x, 2) \cdots, f_n(x, 2).$$

We can factor $f(\cdot, 0)$, $f(\cdot, 1), \ldots,$ using a univariate polynomial factorization algorithm, and try use the collected information to reconstruct a factorization of $f(x, y)$.

This is a very simplified view of the bivariate factoring algorithm, as shown by the following example. Consider the polynomial

$$f(x, y) = x(x + 1) + y^2.$$

This is an irreducible polynomial, i.e., it does not factor. However the univariate polynomial

$$f(x, 0) = x(x + 1)$$

is reducible. So, the factorization of $f(x, 0)$ does not immediately gives a factorization of $f(x, y)$, still it gives useful information. In the following we will introduce a technique called Hensel lifting that will tell us how to extract this information. Notice that factoring univariate polynomial $f(x, 0) = g(x, 0)h(x, 0)$ is equivalent to finding a factorization

$$f(x, y) = g(x, y)h(x, y) \pmod{y}.$$

Hensel's lifting allows us to "lift" factorization modulo (y^k) to factorizations modulo (y^{2k}). This lifting is the central idea in the bivariate factorization algorithms, which we outlined below:

1. Initial preprocessing.
2. (a) Factor $f(x, y) = g(x, y)h(x, y) \pmod{y}$ using a univariate factorization algorithm.

(b) Iteratively "lift" the factorization to obtain

$$f(x,y) = g_k(x,y)h_k(x,y) \pmod{y^k}.$$

3. Cleaning up: Given factors of f modulo y^k, find a non-trivial factorization $f = g.h$

2 Hensel's Lifting Lemma

Hensel's Lemma tell us how to lift a factorization modulo y, to obtain a factorization modulo y^k for any k. For example, given polynomial $f(x,y) = x(x+1) + y^2$ we obtain factorizations

$$\begin{array}{rcl} f & = & x(x+1) \pmod{y} \\ f & = & x(x+1) \pmod{y^2} \\ f & = & (x+y^2)(x+1-y^2) \pmod{y^4} \\ \vdots & & \end{array}$$

One may think of this process as finding approximate roots of polynomial $f_y(x) = f(x,y)$, when y is "small". If $y \approx 0$, than $f_y(-1) \approx 0$ is an approximate solution and $x+1$ is a factor modulo y. A better approximation is $-1+y^2$ which gives the factor $x+1-y^2$ modulo y^4. This is reminiscent of methods from numerical analysis which iteratively try to get closer and closer approximations to a solution for a given equation. Indeed Hensel's lifting is based on such intuition.

Formally, Hensel's Lifting Lemma tell us how to transform a factorization modulo y^k into a factorization modulo y^{2k}. The lemma works for any ideal and can be stated in a very general form. Recall that an ideal is a subset $I \subset R$ of a ring such that

$$\forall x, y \in I,\ \forall \gamma \in R,\ (x+y) \in I`mbox\ and\ \gamma x \in I.$$

Example of ideals are:

- Integral multiples of an integer m: $\mathbb{Z}_m = \{mn : n \in \mathbb{Z}\}$.
- Multiples of a polynomial p.
- The set of bivariate polynomials in x, y with monomials $x^i y^j$ such that $i + j \geq d$.

Ideals are important because we can define the quotient R/I, where $p \equiv q \pmod{I}$ if $p - q \in I$, and operations on R/I are well defined. The *product* of two ideals I, J is the set of all finite sums of products of elements of I and J:

$$I \cdot J = \{\sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J\}.$$

For example, if, for some $p \in R$, I_p is the ideal $\{pq : q \in R\}$ (denoted (p)) then $I^2 = I.I = (p^2)$.

For u.f.d. $f, g, \in R$ and ideal I in R, we say that $\mathrm{pseudo-gcd}(f,g) = 1 \pmod{I}$ to imply that there exist $a, binR$ such that $af + bg = 1 \pmod{I}$. Notice that since R/I is not necessarily a u.f.d., it does not make sense to talk of a real gcd in R/I.

Lemma 1 (Hensel's Lifting) *Let R be a ring and $I \subset R$ be an ideal. For any $f \in R$ and for any factorization $f = gh \pmod{I}$ of f in R/I such that $\mathrm{pseudo-gcd}(g,h) = 1 \pmod{I}$ there exist g^* and h^* such that*

$$\begin{cases} f \equiv g^* h^* \pmod{I^2} \\ g^* \equiv g \pmod{I} \\ h^* \equiv h \pmod{I}. \end{cases} \tag{1}$$

Moreover, the following holds:

- *for any solution* g^*, h^* *to (1),* $\text{pseudo}-\gcd(g^*, h^*) = 1 \pmod{I^2}$ *(ie.* $a^*g^* + b^*h^* \equiv 1 \pmod{I^2}$ *for some* a^*, b^**).*
- *given* a, b, g, h*, one can easily compute* a^*, b^*, g^*, h^**.*
- *The solution* g^*, h^* *is unique in the following sense. Any other pair* g', h' *is a solution to (1) iff*

$$\begin{aligned} g' &\equiv g^*(1+u) \pmod{I^2} \\ h' &\equiv h^*(1-u) \pmod{I^2} \end{aligned}$$

for some $u \in I$*.*

Proof We know that $m \stackrel{\text{def}}{=} (f - gh) \in I$. Let $a, b \in R$ be such that $af + bg = 1 \pmod{I}$. Let

$$\begin{aligned} g^* &\stackrel{\text{def}}{=} g + bm \text{ and} \\ h^* &\stackrel{\text{def}}{=} h + am. \end{aligned}$$

Then g^* and h^* are congruent to g and h modulo I, respectively. Let's check that $f = g^*h^* \pmod{I^2}$:

$$\begin{aligned} f - g^*h^* &= f - (g+bm)(h+am) \\ &= f - gh - m(ag+bh) - abm^2 \\ &= m(1 - (ag+bh)) + abm^2 \\ &\equiv 0 \pmod{I^2} \end{aligned}$$

because $m \in I$ and $ag + bh \equiv 1 \pmod{I}$. This proves that system (1) always has solution.

Now, let g^*, h^* be any solution and let's prove that $\text{pseudo}-\gcd(g^*, h^*) = 1$. Let $q = ag^* + bh^* - 1$. Notice that $ag^* + bh^* \equiv_I ag + bh \equiv_I 1$, and therefore $q \in I$. Define

$$\begin{aligned} a^* &= a - aq \\ b^* &= b - bq \end{aligned}$$

and let's check that $a^*g^* + b^*g^* = 1 \pmod{I^2}$:

$$\begin{aligned} a^*g^* + b^*g^* - 1 &= ag^* + bg^* - 1 - q(ag^* + bg^*) \\ &= q(1 - (ag^* + bg^*)) \\ &= -q^2 \in I^2. \end{aligned}$$

It remains to prove the "uniqueness" of the solution. Clearly, for any $g' \equiv_{I^2} g^*(1+u)$, $h' \equiv_{I^2} h^*(1+u)$ (for $u \in I$), we have $g' \equiv_I g^* \equiv_I g$, $h' \equiv_I h^* \equiv_I h$ and $g'h' \equiv_{I^2} g^*h^*(1-u^2) \equiv_{I^2} f$. Now assume g', h' is a solution to (1). Let $g_1 = g' - g^*$ and $h_1 = h' - h^*$. Since $g' \equiv_I g \equiv_I g^*$ and $h' \equiv_I h \equiv_I h^*$ we have $g_1, h_1 \in I$. Define

$$u = a^*g_1 - b^*h_1.$$

Since $g_1, h_1 \in I$ we also have $u \in I$. We claim that $g' \equiv_{I^2} g^*(1+u)$ and $h' \equiv_{I^2} h^*(1-u)$. For g' we have

$$\begin{aligned} g^*(1+u) &\equiv g^*(1 + a^*g_1 - b^*h_1) \\ &= g^* + a^*g^*g_1 - b^*g^*h_1 \\ &\equiv g^* + (1 - b^*h^*)g_1 - b^*g^*h_1 \\ &= g^* + g_1 - b^*(h^*g_1 + g^*h_1) \\ &\equiv g' - b^*(h^*g_1 + g'h_1) \\ &= g' - b^*(h^*g' - h^*g^* + g'h' - g'h^*) \\ &\equiv g' - b^*(f - f) = g'. \end{aligned}$$

The proof for h' is analogous. ■

When $R = F[x,y]$ is the bivariate polynomial ring and $I = (y^k)$ the "uniqueness" of the solution can be stated in a more expressive way.

Corollary 2 *Let $R = F[x,y]$ and $k \in \mathbb{Z}^+$. Let $f, g, h \in R$, with g monic in x satisfying $f \equiv_{(y^k)} gh$ and $\mathrm{pseudo-gcd}(g,h) = 1 \pmod{y^k}$. Then there exists a unique $g^* \pmod{y^{2k}}$ monic in x such that $g^* \equiv g \pmod{y^k}$ and g^* divides f modulo y^{2k}.*

Proof By Lemma 1 there exists $g^* \equiv g \pmod{I}$ and $h^* \equiv h \pmod{I}$ such that $f \equiv g^* h^* \pmod{I^2}$. We know $g^* - g$ is a multiple of y^k and g is monic in x. Therefore we can apply the division algorithm to divide the polynomial $a \stackrel{\mathrm{def}}{=} (g^* - g)/y^k$ by g and obtain polynomials q and r such that

$$a = qg + r$$

where $deg_x r < deg_x g$. Let $g' = g + y^k r$. Clearly, g' is monic and $deg_x g' = deg_x g$. Moreover, $g' = g^*(1 - y^k q g^*) + y^k q(g^* - g) \equiv_{I^2} g^*(1+u)$ where $u = -y^k q g^* \in I$. It follows from lemma 1 that $f \equiv g'h' \pmod{I^2}$ for $h' = h^*(1-u)$, ie. g' divides f modulo I^2.

This proves that there exists a solution g' such that g' is monic and of degree $\deg_x g$. It remains to prove that the solution is unique. Let $g'' \equiv_I g$ be such that $f = g''h'' \pmod{I^2}$. We have $g''(h'' - h) \equiv_I g''h'' - gh \equiv_I f - f = 0$, ie. $y^k | g''(h'' - h)$. Since g'' is monic in x, this is possible iff $y^k | (h'' - h)$, ie. $h'' \equiv_I h$. We can now apply the uniqueness part of lemma 1 and get $g'' = g'(1+u)$ for some u. Since g'' are both monic of degree $deg_x g$, it must be $g'' = g'$. ■

3 The factoring algorithm

We now give further details of the three steps of the bivariate polynomial factoring algorithm outlined in Section 1.

Let f be the given bivariate polynomial. Our basic idea is to use the univariate factoring algorithm to find a factorization $f(x,y) = g_0(x,y)h_0(x,y) \pmod{y}$. The goal of Step 2 is to lift this factorization to one modulo y^{2^k}. For this we will assume that g_0 is monic and relatively prime to h_0, so as to be able to use Lemma 1. For what follows it will also be useful to know that g_0 is irreducible, so we assume that too. In the next lecture we will show how to get rid of these assumptions by some initial preprocessing in Step 1. (Notice that either of the assumptions (1) g_0 is relatively prime to h_0 or (2) g_0 is irreducible is trivial to achieve; but it is non-trivial to get the two properties together.) Having lifted the factorization for sufficiently large value of k, the main sub-steps of Step 3 of the algorithm are the following:

Step 3(a). Find $\tilde{g}$ and l_k such that

$$\left.\begin{array}{l} \tilde{g} = g_k l_k \pmod{y^{2^k}} \\ \deg_x \tilde{g} < \deg_x f \\ \deg_y \tilde{g} \leq \deg_y f \\ \tilde{g} \neq 0 \end{array}\right\} \qquad (2)$$

Step 3(b). Find $\gcd_x(f,g)$ (viewed as polynomials in $F(y)[x]$) and if non-trivial, a non-trivial factorization of f in $F[x,y]$ may be found using Gauss's Lemma.

The following questions arise:

- How do we know $\tilde{g}$ and l_k satisfying (2) exist?
- How do we find such a pair $\tilde{g}$ and l_k?

- Why does the existence of $\tilde{g}$ and l_k yield anything in Step 3(b)? (The answer to this will also answer the question: "How large should k be?")

We answer these questions in turn. To do so we have to study the properties of the polynomials g_0 and g_k (relative to f). Notice that g_0 does not necessarily correspond to a factor of f. However, g_0 does *divide* (modulo y) an irreducible factor of f. In other words, there exist polynomials $g(x,y), h(x,y)$ such that $f(x,y) = g(x,y)h(x,y)$, $g(x,y)$ is irreducible and $g(x,y) = g_0(x,y)l_0(x,y) \pmod{y}$ and $h_0(x,y) = l_0(x,y)h(x,y) \pmod{y}$. We claim that g forms part of a candidate solution to (2).

Claim 3 *If $f(x,y) = g(x,y)h(x,y)$ for some g and h that are relatively prime; and $g(x,y) = g_0(x,y)l_0(x,y) \pmod{y}$ for some polynomial l_0, then there exists a polynomial l_k such that $\tilde{g} = g$ and l_k form a solution to (2).*

Proof Notice first g satisfies the degree conditions and the condition $g \neq 0$. It suffice to show that there exists l_k such that $g(x,y) = g_k(x,y)l_k(x,y) \pmod{y^{2^k}}$.

We find l_k by applying the Hensel lifting procedure to the factorization of g modulo y. This yields polynomials $\tilde{g}_k$ and l_k such that $g(x,y) = \tilde{g}_k(x,y).l_k(x,y) \pmod{y^{2^k}}$, where $\tilde{g}_k$ is monic in x, and satisfies $\tilde{g}_k = g_0 \pmod{y}$. We claim $\tilde{g}_k = g_k$. To do so we set $\tilde{h}_k(x,y) = l_k(x,y)h(x,y)$ and then notice that

$$f(x,y) = g(x,y)h(x,y) = \tilde{g}_k(x,y)l_k(x,y)h(x,y) \pmod{y^{2^k}} = \tilde{g}_k(x,y)\tilde{h}_k(x,y) \pmod{y^{2^k}}.$$

Additionally $\tilde{g}_k$ is monic and equals $g_0 \pmod{y}$. Thus $\tilde{g}_k$ and $\tilde{h}_k$ satisfy all the properties of the solution to the Hensel lifting procedure after k iterations. But the solution to the Hensel lifting is unique, implying $g_k = \tilde{g}_k$. This yields the claim. ■

Now that we know a solution exists, we can easily find polynomials $\tilde{g}$ and l_k of the required degree just by solving a system of linear equations, where the unknown are the coefficients of $\tilde{g}$ and l_k. This answers the second question above.

Finally, we need to see why computing the greatest common divisor of f and $\tilde{g}$, as polynomials in $F[y](x)$, yields a non-trivial factorization.

Claim 4 *Let g, l_k be any pair of polynomials satisfying (2). Let $2^k > 2d^2$ where d is the (total) degree of f. Then $\gcd_x(f,g)$ is non-trivial.*

Proof Obviously $\gcd(f,\tilde{g}) \neq f$ because $\deg_x g < \deg_x f$. Assume for contradiction that $\gcd_x(f,\tilde{g}) = 1$. Then there exist polynomials $u(x,y)$ and $v(x,y)$ such that

$$u(x,y)f(x,y) + v(x,y)g(x,y) = \mathrm{Res}_x(f,g)$$

where $\mathrm{Res}_x(f,g)$ is the resultant of f and g w.r.t. x. Recall that the resultant is a non-zero polynomial in y of degree at most $2d^2$ (see Lecture 4). Call this polynomial $D(y)$. Using the assumption that $2^k > 2d^2$, we get that $D(y) \neq 0 \pmod{y^{2^k}}$. Thus reducing the equation above modulo y^{2^k} we get

$$\begin{aligned}
D(y) \pmod{y^{2^k}} &= u(x,y)f(x,y) + v(x,y)\tilde{g}(x,y) \pmod{y^{2^k}} \\
&= u(x,y)g_k(x,y)h_k(x,y) + v(x,y)g_k(x,y)l_k(x,y) \pmod{y^{2^k}} \\
&= g_k(x,y)(u(x,y)h_k(x,y) + v(x,y)l_k(x,y) \pmod{y^{2^k}},
\end{aligned}$$

But the above is contradicting. Oh the LHS we have a non-zero element of $F[x,y]$ with degree 0 in x. On the RHS we get either zero (by letting $u(x,y)h_k(x,y) + v(x,y)l_k(x,y) = 0 \pmod{y^{2^k}}$) or we get a term of positive degree in x since g_k is monic in x and has positive degree in x. In either case we are done. ■

In the next lecture we wrap up the above algorithm, by performing the right preprocessing.