Algebra and Computation Course Instructor: V. Arvind

Lecture 14: Bivariate Factorization

Lecturer: V. Arvind *Scribe: Ramprasad Saptharishi*

1 Overview

In the next two lectures, we shall discuss bivariate factorization. We shall look at the major parts of the algorithm, and fill up the missing ends next class.

2 The Idea

We saw last time that for any field F, $F[x, y]$ is a unique factorization domain. And since we know how to factorize univariate polynomials, thinking of $F[x, y]$ as $F(y)[x]$ might be useful.

Assume that f is square-free and that $f(x, 0)$ is square-free as well. Since $f(x, 0)$ is a polynomial in x alone, we know to factorize it. Suppose, $f(x, 0) = g_0(x, 0)h_0(x, 0)$, this can be thought of as a factorization $\pmod y$, i.e

$$f(x, y) = g_0(x, 0)h_0(x, 0) \pmod y$$

The questions now are, can we lift this to a factorization modulo higher powers of y? After we lift it sufficiently, would be able to clean up to get the actual factor of f?

3 Hensel Lifting

The following lemmas form the core of the algorithm. The following notation would make things simpler.

Definition 1. *For two elements $f, g \in R$, and I an ideal of R, we say the pseudo-gcd of f, g is $1 \pmod I$ if there exists $a, b \in R$ such that*

$$af + bg = 1 \pmod I$$

Lemma 2 (Hensel's Lifting Lemma)**.** *Let R be an arbitrary commutative ring with identity with an ideal I. If $f \in R$ can be written as $f = gh \pmod{I}$ such the pseudo-gcd of g and h is 1 modulo I, we can lift this factorization in the following sense: There exists g' and h' and a', b' such that*

$$\begin{aligned} f &= g'h' \pmod{I^2} \\ a'g' + b'h' &= 1 \pmod{I^2} \\ g' &= g \pmod{I} \\ h' &= h \pmod{I} \end{aligned}$$

And further, the following also holds

- *Given a, b, g, h, we can easily compute a', b', g', h'.*
- *The solution g', h' is unique in the sense that if g'' and h'' also satisfy the equations, then*

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

  for some $u \in I$.

Proof. Define $g' = g + bm$ and $h' = h + am$, where $f - gh = m \pmod{I^2}$. Now,

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

As for the pseudo-gcd, let $a' = a + am'$ and $b = b + bm'$ where $m' = 1 - (ag' + bh') \in I$.

$$\begin{aligned} a'g' + b'h' &= (a + am')g' + (b + bm')h' \pmod{I^2} \\ &= (ag' + bh') + m'(ag' + bh') \pmod{I^2} \\ &= 1 - m' + m'(1 - m') \pmod{I^2} \\ &= 1 - m' + m' - m'^2 \pmod{I^2} \\ &= 1 \pmod{I^2} \end{aligned}$$

Now for the uniqueness, suppose g'' and h'' also satisfy the equations, and hence let $g'' - g' = m_1 \in I$ and $h'' - h' = m_2 \in I$. Let $u = m_1 a' - m_2 b' \in I$ since both m_1 and m_2 are in I.

$$
\begin{aligned}
f = g''h'' &= g'h' \pmod{I^2} \\
(g' + m_1)(h' + m_2) &= g'h' \pmod{I^2} \\
\implies m_1h' + m_2g' &= 0 \pmod{I^2} \\
\implies m_2g' &= -m_1h' \pmod{I^2} \\
a'm_2g' &= -a'm_1h' \pmod{I^2} \\
m_2(1 - b'h') &= -m_1a'h' \pmod{I^2} \\
m_2 &= h'(m_2b' - m_1a') \pmod{I^2} \\
m_2 &= h'(-u) \\
\implies h'' &= h'(1 - u)
\end{aligned}
$$

and similarly for g''. □

In our context, when $R = F[x, y]$ and $I = \langle y^k \rangle$, if we force g to be monic in x, then we can force the u in the above lemma to be zero.

Lemma 3. *When $R = F[x, y]$ and $I = \langle y^k \rangle$, if $f = gh \pmod{y^k}$ such that g is monic in x. Then we can hensel lift this to g', h' such that the conditions hold and that g' is monic. Infact, g' is unique modulo y^{2k}.*

Proof. By the earlier lemma, there exists a lifting $f = g'h' \pmod{y^{2k}}$. And since $g' - g$ is a multiple of y^k, let $a = (g' - g)/y^k$. Since g is monic in x, we can apply the division algorithm to divide a by g to obtain

$$a = gq + r$$

with $\deg_x r < \deg_x g$. Now let $g_0 = g + ry^k$, another monic polynomial. It is easy to see that $g_0 = g'(1 + u)$ where $u = -y^k qg' \in I$ and hence $g_0, h_0 = h'(1 - u)$ is a solution wiht a monic g_0.

As for uniqueness, any solution looks like $g'' = g'(1 + vy^k)$ for some v, and hence the only way g'' can be monic is when v is zero, and hence g' is unique. □

4 The Factoring Algorithm

1. Preprocess such that f and $f(x, 0)$ are square free. Let the total degree of f be d.

2. Using the univariate factoring algorithm, factorize

$$f(x,y) = g_0(x,y)h_0(x,y) \pmod{y}$$

where g_0 is monic in x and irreducible.

3. Do a hensel lift k times where k is chosen such that $2^k > 2d^2$. Let $f(x,y) = g_k(x,y)h_k(x,y) \pmod{y^{2^k}}$

4. Solve, as a system of linear equations, for

$$g' = g_k(x,y)l_k(x,y) \pmod{y^{2^k}}$$

where $\deg_x g' < \deg_x f$ and $\deg_y l_k, \deg_y g' \leq \deg_y f$.

5. Compute $\gcd_x(f, g')$, as polynomials in $F(y)[x]$, and find a non-trivial factor using Gauss's Lemma if the gcd is non-trivial.

We need to argue that step 4 will have a non-trival solution, and also that hence 5 will happen.

4.1 Step 4 will have a non-trivial solution

Note that when we start with $f = g_0h_0 \pmod{y}$, g_0 need not correspond to a factor of f but will certainly divide a factor modulo y. Let this irreducible factor was called g, and $f = gh$ in $F[x,y]$. Then $g = g_0l_0 \pmod{y}$, where g_0 is monic in x. Hensel lift this k times to obtain $g = g'_k l'_k \pmod{y^{2^k}}$ with $g_0 = g'_k \pmod{y^{2^k}}$ and g'_k monic. We will show that $g'_k = g_k$, the polynomial got by hensel lifting $f = g_0h_0$ for k times.

$$f = gh = g'_k l'_k h = g'_k h' \pmod{y^{2^k}}$$

where $h' = l'_k h \pmod{y^{2^k}}$. But since g'_k is also monic, the hensel lifting is unique and hence $g'_k = g_k$. Thus, $g' = g$ and $l_k = l'_k$ form a non-trivial solution to step 4. □

4.2 Step 5 will happen

Suppose $\gcd_x(f, g') = 1$, then there exists polynomials u, v in $F(x)$ such that

$$uf + vg' = 1$$

Note that the u, v are from $F(x)$, elements from the fraction field. We shall now see how to clear the denominators. Recall that the Sylvester

matrix is the transformation that takes (s,t) to $sf+tg'$. Hence The sylvester matrix would take (u,v) to $uf+vg'=1$. Now, we can use Cramer's rule to hence solve for $\mathcal{S}(u,v)^T=(0,0,\cdots,0,1)^T$. And notice that the denominator for each coordinate in (u,v) would be $Res_x(f,g')$ and hence multiplying each coordinate by that value would completely clear the denominators.

Hence, we can get

$$u'f+v'g=Res_x(f,g')$$

where $u',v'\in F[x,y]$. Going mod y^{2^k}, we have

$$Res_x(f,g')=u'g_kl_k+v'g_kh_k=g_k(u'l_k+v'h_k)$$

Note that the left hand side is of degree atmost $2d^2$ by the choice of k and would remain unchanged when we go modulo y^{2^k}. But the right hand side on the other hand, g_k is monic. The resultant is a polynomial in y alone, and hence the only way the top x in g_k can be killed is when $u'l_k+v'h_k=0$ but that would force $Res_x(f,g')=0$, which contradicts the assumption that $\gcd(f,g')=1$.

Hence step 5 would give us a non-trivial factor of f. □

5 Missing Pieces

The algorithm relies on the assumption that $f=gh$ where g and h are coprime, similarly $f=g_0h_0 \pmod{y}$. Hence, we need the assumption that f and $f(x,0)$ are square free.

We shall fill in these missing ends in the next lecture, and also some interpretations of Hensel Lifting to Newton's method for finding roots.