LECTURE 11

3/14/2012

Note Title 3/13/2012

Today: • Bivariate Factorization

• Few words on (blackbox) multivariate factorization.

Recall algorithm

SPLIT($f \in \mathbb{F}[x,y]$, $\deg(f) = d$)

① - if $\frac{\partial f}{\partial x} = 0$ & $\frac{\partial f}{\partial y} = 0$ then $f = g^p$

else { if $\frac{\partial f}{\partial x} = 0$ $f(x,y) \leftarrow f(y,x)$

if $g = \gcd(f, \frac{\partial f}{\partial x}) \neq 1$ return

$(g, \frac{f}{g})$ }

/* f has no repeated factors */

(1) Pick β s.t. $f(x,\beta)$ has no repeated factors.;

$f(x,y) \leftarrow f(x, y+\beta)$

(2) FACTOR $f = g_1 \cdot g_2 \cdots g_k \pmod{y}$

$= g \cdot h$

(3) LIFT $f = g^{(t)} \cdot h^{(t)} \pmod{y^t}$

$g^{(t)} = g \pmod{y}$

$h^{(t)} = h \pmod{y}$

(4) JUMP $g^{(t)} \to \tilde{g}$ by solving

$\tilde{g} = g^{(t)} \cdot \tilde{h} \pmod{y^t}$

$\deg(\tilde{g}) \le d$; $\deg_x \tilde{g}$ minimal

(5) Return $\left(\tilde{g}, \frac{f}{\tilde{g}}\right)$

Analysis

- Why does $\tilde{g}$ divide f?

Notations:

Let $f = f_1 \cdot f_2 \cdot \cdots f_\ell$, f_i irred.

Let $f_i = f_{i1} \cdot f_{i2} \cdots f_{in_i} \pmod y$

Claim 1: $k = \sum_{i=1}^{\ell} n_i$ &

$\{f_{i1}, \ldots f_{in_i}\}_{i=1}^{\ell} \equiv \{g_1 \ldots g_k\}$

(Proof, Obvious by Unique factorization)

Claim 2: if $g_1 = f_{ij}$ for some i, j

then $g = f_i$ for same i

Proved via Claims below ...

Claim 2.1: If we lifted

$$f_i = \underbrace{f_{ij}}_{g} \cdot \underbrace{\left(\prod_{m \neq j} f_{im}\right)}_{h_0} \pmod{y}$$

$$\Downarrow$$

$$f_i = g_0^{(t)} \cdot h_0^{(t)} \pmod{y^t}$$

Then $\exists\, U \in \mathbb{F}[x,y]$ s.t.

$$g^{(t)} = g_0^{(t)} \left(1 + U \cdot y^{t/2}\right) \pmod{y^t}$$

$$\Leftrightarrow \quad g^{(t)}\left(1 - U y^{t/2}\right) = g_0^{(t)} \pmod{y^t}$$

Proof: by uniqueness of H-L., since

$$g_0^{(t)} \cdot \underbrace{h_0^{(t)} \cdot \prod_{m \neq i} f_m}_{} = f \pmod{y^t}$$

$$g^{(t)} \cdot h^{(t)} = f \pmod{y^t}$$

$\square$

$\exists \tilde{h}_0$ s.t.

Claim 2.2: $(f_i, \tilde{h}_0)$ is a valid solution to the jump problem (ignoring minimality)

Proof: We have

$$f_i = g_0^{(t)} \cdot h_0^{(t)} \pmod{y^t}$$

$$= \underbrace{g^{(t)}}_{\tilde{g}} \cdot \underbrace{h_0^{(t)} \cdot (1 - v y^{t/2})}_{\tilde{h}_0} \pmod{y^t}$$

$\square$

Claim 2.3: Let $(\tilde{g}, \tilde{h})$ be any minimal solution to jump problem. Then $\tilde{g}, f_i$ share common factor; and so $\tilde{g} \sim f_i$

Proof: Assume $\tilde{g}, f_i$ have no common factor. Then their resultant $R(y) = \mathrm{Res}_x(\tilde{g}, f_i)$ is non-zero,

of degree at most d^2, and is in the ideal of $(\tilde{g}, f_i)$

$$R(y) = A \cdot \tilde{g} + B \cdot f_i$$

$$= A \cdot g^{(t)} \cdot \tilde{h} + B \cdot g^{(t)} \cdot \tilde{h}_0 \pmod{y^t}$$

$$= g^{(t)} \left(A \cdot \tilde{h} + B \cdot \tilde{h}_0 \right) \pmod{y^t}$$

$g^{(t)}$: monic in x

$A \cdot \tilde{h} + B \cdot \tilde{h}_0$: consider highest deg. term in x; can't vanish!