LECTURE 08 3/5/2012

Note Title 2/28/2012

TODAY

1. Deterministic Factorization over $\mathbb{F}_{p^k}$
2. Factorization of Bivariate Polynomials.

—— ∞ ——

Deterministic Factorization:

Key idea: to factor $f = f_1 \cdot f_2$ irred., deg d.

- $\exists$ non-trivial poly g s.t.

$$g(x)^p - g(x) \equiv 0 \pmod{f}$$

- $$g(x)^p - g(x) = \prod_{\alpha \in \mathbb{F}_p} (g(x) - \alpha)$$

  helps factor f

- Can find such g efficiently by linear algebra.

I. Existence of g.

Defn: g non-trivial if $0 < \deg g < \deg f$.

① $\exists$ trivial g

e.g. $g(x) = \alpha \in \mathbb{F}_p$

② Suffices to have

$$g(x)^p - g(x) = 0 \mod f_1$$
$$g(x)^p - g(x) = 0 \mod f_2$$

③ Now use

$$\left.\begin{aligned} g(x) &= \alpha \mod f_1 \\ g(x) &= \beta \mod f_2 \end{aligned}\right\} \text{exists by CRT}$$

$g \notin \mathbb{F}_q$ since $g^p = g$ only for $g = \alpha \in \mathbb{F}_p$

$\deg g < \deg f$ (else use $g \pmod f$)

III. Finding g

- <u>Idea</u>: Should be easy since set of all (trivial + non-trivial) solutions form $\mathbb{F}_p$ - vector space.

g, h satisfy

$$g^p - g = 0 \mod f$$
$$h^p - h = 0 \mod f$$
$$\Downarrow$$
$$(g+h)^p - (g+h) = 0 \mod f$$

- Can we find the constraints explicitly over $\mathbb{F}_p$?

- Representations of $\mathbb{F}_q = \mathbb{F}_{p^t}$?
  - Represent by t linearly independent el'ts

$$\alpha_1 \ldots \alpha_t \in \mathbb{F}_q$$

  - Along with multiplication identities

$$\alpha_i \cdot \alpha_j = \sum \gamma_{ijk} \alpha_k \qquad \gamma_{ijk} \in \mathbb{F}_p$$

- $g = ?$

$$g(x) = \sum_{i=0}^{2d-1} \left(\sum_{j=1}^{t} c_{ij} \alpha_j \right) x^i$$

$$c_{ij} \in \mathbb{F}_p$$

- $g^p = ?$

$$g(x)^p = \sum_{i=0}^{2d-1} \left(\sum_{j=1}^{t} c_{ij} \alpha_j^p \right) x^{ip}$$

- Reducing $x^{ip} \pmod f$ & $\alpha_j^p \to \sum \delta_{jk} \alpha_k$ are linear maps... can be computed explicitly.

- Coefficient of x^{ℓ} in $g^{p} - g \pmod f$ is linear function of c_{ij}; can be computed efficiently;
  (helps to precompute;
$$\alpha_i^{p} = \sum_{j} \delta_{ij} \alpha_j \qquad \delta_{ij} \in \mathbb{F}_p$$
$$x^{e} = \sum_{i=0}^{2d-1} \left(\sum_{j=0}^{2d-1} \beta_{ij} f_j \right) x^{i} \qquad \beta_{ij} \in \mathbb{F}_q$$
where $f = \sum f_j x^j$)

- Thus g can be solved by solving linear system over $\mathbb{F}_p$

II. Final Factorization Algorithm

Step 1: Find non-trivial g s.t.

$$g^p - g = 0 \pmod f$$

Step 2: for $\alpha \in \mathbb{F}_p$

if $\gcd(f, g-\alpha) =$ non-trivial

report $\left(\gcd, \frac{f}{\gcd}\right)$;

Claim: $f \mid g^p - g \Rightarrow \exists \alpha \in \mathbb{F}_p$

s.t. $\gcd(f, g-\alpha)$ is non-trivial

Proof: Obvious

Upcoming Lectures

- Factoring Bivariate Polynomials
- Factoring Rational Polynomials

Common Theme

Input: Polynomial $f \in R[x]$

$(R = \mathbb{F}[y] \quad \text{or} \quad R = \mathbb{Z})$

Plan:
- Find ideal $I \in R$
- Perturb f
- Factor $f \pmod{I}$ [hopefully easy]
- Hensel Lifting
  Factor $f \pmod{I^t}$ for large t
- "Jump" to actual factorization.

Details :

① The Ideal : $I = (y)$ if $R = \mathbb{F}[y]$

$= (p)$ if $R = \mathbb{Z}$

↑ prime

Good News : In both cases easy to factor in $R[x]/I$

Aside : R/I the "quotient" ring :

Always well defined ;

- Elements of $R/I = a + I,\ a \in R$

- Sum / Product as natural

$$(a+I) + (b+I) = (a+b) + I$$

$$(a+I)\cdot(b+I) = ab + I$$

↑ "closed under R mult"

This is what we used to create extension fields

Last Step : The Jump ?

- What does it do? Why?
- To understand we need to understand what could happen at first step.
- Suppose $f = f_1 \cdot f_2 \cdot f_3 \cdots f_k$ in $R[x]$

1 - Can f have fewer factors in $R[x]/I$?

2 - Can f have more factors in $R[x]/I$?

Answers : YES (1) & YES (2).

YES (1) } ⇒ Some $f_i \pmod{I}$ may become constants.

(e.g. $f_i = \alpha + p \cdot g(x)$

$\alpha + y \cdot g(x)$)

But a rare event .... will have to prove; prevent by perturbing.

$f \in \mathbb{F}_p[x,y]$

YES ② $\Rightarrow$ e.g. $f(x,y) = x^p - x + y \cdot g(x,y)$

$\uparrow$ random.

f is probably irreducible but factors completely (mod y).

- Hensel Lifting?

$$f = f_1 \cdot f_2 \cdot \cdots f_p \pmod{I}$$

$$f = f_1' f_2' \cdots f_p' \pmod{I^t}$$

Will lift whenever conditions are good.

- So need to use f_1' to find some non-trivial irreducible factor of f.

- Modulo some math
  - $\Rightarrow$ linear algebra in $\mathbb{F}[x,y]$.
  - $\Rightarrow$ lattice reduction in $\mathbb{Z}[x]$.

Some Math

- Why should f_1 give info on factors of f?
  - Suppose $f = g_1 \cdot g_2 \cdot g_3 \cdots g_\ell$
  - $f_1 \ldots f_k$ are (if we're lucky) factorizations of $g_1 \ldots g_\ell \pmod{I}$.
  - So f_1 comes from one of the g_i's say g_1

- What do we know about g_1
  - factor of f
  - has f_1' as factor modulo I^t
  - has degree $< \deg(f)$
  - coefficients of g_1 small if coeff. of f are small.

PROBLEM: Given $h \in \mathbb{F}[x,y]$ of deg D

find $g \in \mathbb{F}[x,y]$ of deg d s.t.

$\exists\, \tilde{g}$ s.t. $g = \tilde{g} \cdot h \pmod{y^2}$

SOLUTION: linear algebra

given $\tilde{g}$, g is a linear form

in coefficients of $\tilde{g}$.

- Does this really solve the problem?
- Will $g = g_1$ that we care about?
- Will defer proof, but answer is YES

Integer version

Problem: Given $h \in \mathbb{Z}[x]$, N find $g \in \mathbb{Z}[x]$ with "small" coefficients s.t. $\exists\ \tilde{g} \in \mathbb{Z}[x]$ s.t.

$$g = \tilde{g} \cdot h \pmod{\underset{\underset{p^t}{\shortparallel}}{N}}$$

Solution: "Short vector in lattice problem".

- Set of solutions form a lattice in $\mathbb{Z}^{d+1}$

$(g_{(0)}, \tilde{g}_{(0)})$ & $(g_{(1)}, \tilde{g}_{(1)})$ are solutions

$\Rightarrow (g_{(0)} + g_{(1)}, \tilde{g}_{(0)} + \tilde{g}_{(1)})$ is solution

- if $h = \sum h_i x^i$ & $g = \sum g_i x^i$, then lattice spanned by columns of

$$\left[\begin{array}{cccc|cccccc}
h_0 & & & 0 & N & & & & & 0 \\
h_1 & h_0 & & & & N & & & & \\
\vdots & h_1 & & & & & N & & & \\
h_k & \vdots & & h_0 & & & & N & & \\
 & h_k & & & & 0 & & & N & \\
0 & & \ddots & h_k & & & & & & N
\end{array}\right]$$

Main Questions: (in lin. algebra / lattice)

- Why does appropriate g exist?
- if it exists is it unique, or will all g exist?

Usual answers

- Solution exists because the irreducible factor we are looking for satisfies all criteria
- Solution is not unique
- "Any solution of minimum x degree will do."

This needs formalization + proof.

"Uniqueness" Lemmas

Lemma ($\mathbb{F}[y]$): Let $h \in \mathbb{F}[x,y]$ with $\deg(h) \leq d$.
$(a, \tilde{a})$ & $(b, \tilde{b})$ be two sets of solution to $(g, \tilde{g})$ in system below

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

$$\deg_y(g) \leq d \,;$$

Furthermore let a be solution of smallest x degree. Then, if $t \geq ???$,
$a \mid b$.

(So, in our case, if b is the solution we desire & a is the solution we find of min. degree, then $a \sim b$.)

Lemma ($\mathbb{Z}$): Let $h \in \mathbb{Z}[x]$ with $|\text{coeff.}| \leq M_0$ & $\deg(h) \leq d$.

Let $(a, \tilde{a})$ & $(b, \tilde{b})$ be solutions to

$$g = \tilde{g} \cdot h \mod N$$

$$|\text{coeffs of } g| \leq M_1$$

Then if $\deg_x(a)$ is smallest possible,

& $N > N(M_0, M_1)$ then $a | b$

Proofs: Need to 1 introduce Resultants

& 2 bound coeff. of factors.

Boring Part: Bounding Coefficients 2

Lemma: Let $a = \sum a_i x^i$ divide $b = \sum_{i=0}^{d} b_i x^i$

Then if $|b_i| \le 2^n$, $|a_j| \le 2^{n\,\mathrm{poly}(d)}$

$[a_i, b_j \in \mathbb{Z}]$

Sublemma 1: All complex roots of $b = \sum b_i x^i$ bounded by $B = \max_i \{1 + |b_i|\}$

Proof:

$$b_n \cdot B^n \geq B^n > \max_{i<n} |b_i| \cdot \sum_{i=0}^{n-1} B^i$$

$$\geq \sum |b_i| B^i,$$

so B can't be a root.

Sublemma 2: if all complex roots of $a = \sum_{i=0}^{m} a_i x^i$ are bounded by B, then $\left|\frac{a_i}{a_m}\right| \le 2B^m$

Proof: follows since coefficients are the symmetric polynomials in roots, mult. by a_m

Lemma follows.

Back to Uniqueness Lemmas

How to prove $a \mid b$?

- Actually we'll try to prove $\gcd(a,b) \neq$ non-trivial
- take the case where $a, b \in \mathbb{F}[x,y]$
- view them as elements of $\mathbb{F}(y)[x]$.
- if they don't have a common factor (of pos. degree in x) then

  $\exists\, u, v \in \mathbb{F}(y)[x]$ s.t.

  $$u \cdot a + v \cdot b = 1$$
- Clearing denominators we get

  $\exists\, \bar{u}, \bar{v} \in \mathbb{F}[x,y]$ & $R \in \mathbb{F}[y]$

  s.t. $\bar{u} \cdot a + \bar{v} \cdot b = R$
- Degree of $R = ?$

(Detour)

RESULTANTS!

- Low-degree polynomial in ideal generated by a, b
- Specifically if a, b relatively prime in $\mathbb{F}[x,y]$

  then $R \in \mathbb{F}[y]$ of degree $\deg(a) \cdot \deg(b)$

Definition: $a, b \in R[x]$ of degree k, ℓ respectively. Let $a = \sum a_i x^i$ & $b = \sum b_i x^i$.

Let

$$M(a,b) = \left[\begin{matrix} \underbrace{\begin{matrix} a_0 & 0 & & \\ a_1 & a_0 & \ddots & \\ \vdots & a_1 & \ddots & a_0 \\ a_k & \ddots & & \vdots \\ \vdots & a_k & & \vdots \\ \vdots & & & \\ & & & a_k \end{matrix}}_{\ell} & \begin{matrix} b_0 & & \\ b_1 & \ddots & \\ \vdots & & b_0 \\ b_\ell & & \vdots \\ & \ddots & \vdots \\ & & \\ & & b_\ell \end{matrix} \end{matrix}\right]$$

Then $\mathrm{Res}_x(a,b) \triangleq \text{determinant}(M(a,b))$

Note: $\mathrm{Res}_x(a,b) \in R$

Motivation

- a & b have common factor $g \in R[x]$ of positive degree in x $\Longleftrightarrow$ there exists a solution to $u, v \in R[x]$ s.t. ① $u \cdot a + v \cdot b = 0$

  ② $\deg(u) < \deg(b)$; $\deg(v) < \deg(a)$

- Writing $u = \sum_{j=0}^{l-1} u_j x^j$ & $v = \sum_{j=0}^{k-1} v_j x^j$ and solving for the unknowns, we are solving

$$M(a,b) \begin{bmatrix} u_0 \\ \vdots \\ u_{l-1} \\ v_0 \\ \vdots \\ v_{k-1} \end{bmatrix} = \begin{bmatrix} \\ 0 \\ \\ \end{bmatrix}$$

for a non-zero solution.

- Solution exists iff $\mathrm{Res}(a,b) = 0$.

Properties of resultant

① $\mathrm{Res}(a,b) \in \mathrm{Ideal}(a,b)$

Claim 1: $\forall\, M \in R^{n\times n}$, the vector $\begin{pmatrix} \mathrm{Det}(m) \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ is in the column span of M.

Proof: Can do column operations of M to convert it to $\begin{bmatrix} g_1 & & & 0 \\ & g_2 & & \\ ? & & \ddots & \\ & & & g_n \end{bmatrix}$ s.t.

$\det(m) = \prod_i g_i$. Can now generate $\begin{pmatrix} \det(m) \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ from above by taking some R-linear combinations.

Claim 1: $\Rightarrow$ ① immediately

② $\mathrm{Res}(a,b)$ is poly in coeff of a, b of deg $\le \deg(a) + \deg(b)$

②' $a, b \in \mathbb{F}[x,y]$ with $\deg(a) = k$, $\deg(b) = l$

$\Rightarrow \mathrm{Res}_x(a,b)$ is poly of deg $k \cdot l$ in y

Proof: Careful counting.

$$\deg(M(a,b))_{ij} \le k - i + j \quad \text{if } j \le l$$
$$\le j - i \quad \text{if } j > l$$

Thus $\forall$ permutations σ

$$\deg\left(\prod_j M(a,b)_{\sigma(j)j}\right) \le kl$$

Lemma: $a, b \in \mathbb{F}[x,y]$ of deg $\le k, l$ resp. with no common factor of degree > 0 in $x \Rightarrow \exists R(y)$ of deg $\le k \cdot l$ in $I(a,b)$

Proof: Resultant.

Applications of Resultants

Bezout's Theorem (weak form, in the plane)

$a, b \in \mathbb{F}[x,y]$ have $> k \cdot l$ common points

$\Rightarrow$ a, b have common factor.

Proof: • Let $t = k \cdot l + 1$ & let

$(\alpha_1, \beta_1) \; \ldots \; (\alpha_t, \beta_t) \in \mathbb{F} \times \mathbb{F}$ be

t common zeroes.

• By affine-coordinate transform, can assume β_i's are all distinct. (work over $\overline{\mathbb{F}}$ if needed)

• Every poly in $I(a,b)$ vanishes at $(\alpha_1, \beta_1) \; \ldots \; (\alpha_t, \beta_t)$.

• if no common factor, $\mathrm{Res}(a,b) = R(y)$ is zero at $\beta_1 \ldots \beta_t$

• Contradicts $\deg(R) < t$. $\boxtimes$

Application 2: Repeated factors

Lemma: If $f \in \mathbb{F}[x,y]$ is square-free

(no g s.t. $g^2 \mid f$)

then $\left|\{\beta \in \mathbb{F} \mid f(\cdot,\beta) \text{ has square factor}\}\right| \le d^2$

Proof: • f is square-free $\Leftrightarrow$ (f, f') have no common factor.

$\Leftrightarrow$ $\Delta = \mathrm{Disc}(f) \triangleq \mathrm{Res}_x(f, f') \neq 0$

• $\Delta \in \mathbb{F}[y]$ of deg $\le d^2$

• Similarly $f_\beta \triangleq f(\cdot,\beta)$ is square-free

iff $\mathrm{Disc}(f_\beta) \neq 0$

But $\mathrm{Disc}(f_\beta) = \Delta(\beta)$

$\boxtimes$

BACK TO UNIQUENESS LEMMA (PAGE 15)

Lemma: $(a, \tilde{a})$, $(b, \tilde{b})$ satisfy

$$a = \tilde{a} \cdot h \pmod{y^t};$$

$$b = \tilde{b} \cdot h \pmod{y^t};$$

$$\deg(a, b) \leq d;$$

& a irreducible
& $t > d^2$ $\Big\} \Rightarrow a \mid b$

Proof: Assume $a \nmid b$. Then $\exists\, u, v \in \mathbb{F}[x,y]$

s.t. $a \cdot u + b \cdot v = R = \mathrm{Res}_x(a,b) \in \mathbb{F}[y] \setminus 0$

$\Rightarrow \tilde{a} \cdot h \cdot u + \tilde{b} \cdot h\, v = R = 0 \pmod{y^t}$

But R is non-zero & of degree $\leq d^2 < t$

$\Rightarrow R \not\equiv 0 \pmod{y^t}$

$\boxtimes$

$\mathbb{Z}[x]$ version similar; argue about size of R as opposed to degree.

HENSEL LIFTING

- Will describe process first; see what it needs to work & will get lemma later. Structure of lemma below

"Lemma": Let $I \subseteq R$ be an ideal.

- Let $f, g, h \in R[x]$ satisfy
$$f = g \cdot h \pmod{I}$$
- Then under some conditions on g, h the factorization can be lifted, i.e.,

  ?

$$\exists\ \tilde{g}, \tilde{h} \qquad \tilde{g} = g \pmod{I}\ ;\ \tilde{h} = h \pmod{I}$$
$$\&\quad f = \tilde{g} \cdot \tilde{h} \pmod{I^2}.$$
- Such $\tilde{g}, \tilde{h}$ can be found efficiently.
- They are unique in some sense

  ?

Conditions?

Suppose $f = g \cdot h - r$ $\quad\quad r \in I$

$\tilde{g} = g + g_1 r$, $\quad \tilde{h} = h + h_1 r$,

$$\tilde{g} \cdot \tilde{h} = g \cdot h + r(g_1 h + h g_1) + r^2 (g_1 h_1)$$

$$= f + r(1 + g_1 h + h g_1) + r^2 g_1 h_1$$

$$= f + r(1 + g_1 h + h_1 g) \pmod{I^2}$$

Would like to pick g_1 s.t.

$$g_1 = -(h_1 g + 1) \cdot h^{-1} \pmod{I}$$

Does h have inverse (mod I)?

Will make it a precondition, but now will also be post condition. $\tilde{h}$ will be invertible.

Uniqueness of lifts?

- Can't be unique! I can add arbitrary elements of I^2 to $\tilde{g}, \tilde{h}$.
- Also if $\tilde{g}, \tilde{h}$ are solutions, so are $\tilde{g}(1+u)$, $\tilde{h}(1-u)$ for $u \in I$.
- Essentially above are the only things that can happen.

Hensel Lifting Theorem

- R commutative ring, $I \subseteq R$ ideal
- $f, g, h \in R[x]$ s.t. $f = g \cdot h \pmod{I}$
- g, h relatively prime, i.e.,

  $\exists\, a, b \in R[x]$

  s.t. $a \cdot g + b \cdot h = 1 \pmod{I}$

Then

- $\exists\, \tilde{g}, \tilde{h}, \tilde{a}, \tilde{b}$, $\tilde{g} = g \pmod{I}$, $\tilde{h} = h \pmod{I}$

  s.t. $f = \tilde{g} \cdot \tilde{h} \pmod{I^2}$

  $\tilde{a}\tilde{g} + \tilde{b}\tilde{h} = 1 \pmod{I^2}$

- $\tilde{g}, \tilde{h}$ are essentially unique i.e., if

  $g_1 \cdot h_1 = f \pmod{I^2}$ & $g_1 = g \pmod{I}$

  $h_1 = h \pmod{I}$

  then $\exists\, u \in I$ s.t.

  $g_1 = \tilde{g}(1+u)$ & $h_1 = \tilde{h}(1-u)$

[Proof = Exercise]

Bivariate Factorization

Input: $f \in R[x,y]$ of deg d

Goal: find non-trivial split of f.

Alg: 0. If $\gcd(f, f')$ non-trivial, report gcd. & stop.

1. Pick $\beta \in R$ at random & factor $f_\beta = f(x, y+\beta)$ instead

2. Factor $f_\beta = g_\beta \cdot h_\beta \pmod{y}$ s.t. g_β, h_β relatively prime
   if can't find such split, abort.

3. Lift $\log t = \log d^2$ times to get $f_\beta = \bar{g}_\beta \cdot \bar{h}_\beta \pmod{y^t}$

4. Jump from $\bar{g}_\beta$ to g_0 irreducible s.t. $g_0 \mid f_\beta$

$\boxtimes$