Bivariate factoring

- *Idea*: • Given $f \in \mathbb{F}[x,y]$, view it as a univariate over $\mathbb{F}(y)$ & factor it by *fixing* y in $\mathbb{F}$.
  - Say, we factored $f(x,0) = g_0 \cdot h_0$ in $\mathbb{F}[x]$. Can we *recover* factors of $f(x,y)$?
  - View this as $f(x,y) \equiv g_0 \cdot h_0 \pmod{y}$, & *lift* this factorization $\pmod{y^2}$, $\pmod{y^4}$, ...

    compare this with rational approx. of $\sqrt{2}$ or reals!

- The algebraic tool is:

Lemma (Hensel lifting, 1897): Let R be a commutative ring & I be an ideal. If $f, g, h \in R$ s.t.

$f \equiv g \cdot h \pmod{I}$ [I.e. factors mod I) and $\exists a, b \in R$, $ag + bh \equiv 1 \pmod{I}$

[I.e. g, h are "coprime" mod I]

then, we can compute $g', h', a', b' \in R$ s.t.

$(g', h') \equiv (g, h) \pmod{I}$ [i.e. g', h' are <u>lifts</u>]

$$\& \begin{cases} f \equiv g' \cdot h' \pmod{I^2} \\ 1 \equiv a'g' + b'h' \pmod{I^2}. \end{cases}$$

Moreover, g' & h' are <u>unique</u> up to units.

<u>Proof:</u>

- Consider $m := f - gh$.
- A natural lift would be by the multiples of m: $(g', h') = (g + bm, h + am)$.

$$\Rightarrow f - g'h' \equiv f - (g+bm)\cdot(h+am)$$
$$\equiv m - (ag+bh)\cdot m \pmod{I^2}$$
$$\equiv 0 \pmod{I^2}.$$

- Consider now $m' := 1 - (ag' + bh')$. A natural lift of a, b is by the multiples of m':

$$(a', b') = (a + am', b + bm').$$

$$\Rightarrow a'g' + b'h' \equiv (ag' + bh')\cdot(1+m') = (1-m')(1+m')$$

$\equiv \quad 1 - m'^2 \quad \equiv 1 \pmod{I^2}$.

- Suppose g'', h'' are <u>other</u> lifts of g, h.
- Let $(m_1, m_2) = (g'' - g', h'' - h')$. $[m_1, m_2 \in I]$

$\Rightarrow f \equiv g'' \cdot h'' \equiv g' \cdot h' \pmod{I^2}$.

$\Rightarrow (g' + m_1) \cdot (h' + m_2) \equiv g' \cdot h' \pmod{I^2}$

$\Rightarrow m_2 \cdot g' \equiv -m_1 \cdot h' \pmod{I^2}$

- On multiplying by a', we get

$m_2 \cdot (1 - b'h') \equiv -m_1 \cdot a'h' \pmod{I^2}$

$\Rightarrow m_2 \equiv h' \cdot (b'm_2 - a'm_1) \pmod{I^2}$

$\Rightarrow h'' \equiv h' \cdot (1+u) \pmod{I^2}$ $[u := b'm_2 - a'm_1]$

- Since $u \in I$, $(1+u)$ is a <u>unit</u> mod I^2.
- Similarly, for g''.

$\because (1+u)(1-u) \equiv 1 \bmod I^2$ $\square$

- In our current context, $R = \mathbb{F}[x,y]$ & $I = (y^k)$.

We can strengthen the <u>uniqueness</u> conclusion by starting with a <u>monic</u> g.
(i.e. leading coeff. is 1)

<u>Corollary</u>: If $f \equiv g \cdot h \pmod{y^k}$ s.t. $ag + bh \equiv 1 \pmod{y^k}$

& g is monic in x, then we can lift it to $g', h', a', b' \pmod{y^{2k}}$ s.t. g' is monic in x & <u>unique</u>.

<u>Proof</u>:

- We can compute G, H s.t. $f \equiv G \cdot H \pmod{y^{2k}}$, by Hensel lemma.
- If G is <u>not</u> monic wrt x then correct it to $g' := g + r y^k$, where r is the <u>remainder</u> in $(G-g)/y^k = q \cdot g + r$. ← Division by monic g

Note: $\deg_x r < \deg_x g$

[G is non-monic only because of y^k-multiples.]

$\Rightarrow$ g' is monic wrt x.

- Also, $g' = g + (G - g - q \cdot g \cdot y^k) = G - q \cdot g \cdot y^k$

$$\equiv G - q \cdot G \cdot y^k \pmod{y^{2k}}$$

$$\equiv G \cdot (1 - q y^k)$$

- So, picking $h' := H \cdot (1 + q y^k)$ yields:

$$f \equiv g' \cdot h' \equiv G \cdot H \pmod{y^{2k}}.$$

- Uniqueness of g' follows from Hensel lemma & the fact that the units mod y^{2k} are of the form

$\alpha + y\cdot F$, where $\alpha \in \mathbb{F}^*$, $F \in \mathbb{F}[x,y]$.

(Exercise.)

- This, together with the fact that g' is monic wrt x, makes g' unique.

$\square$

— Hensel lifting at work:

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

$$f \equiv x\cdot(x+1) \pmod{y}$$
$$\equiv x\cdot(x+1) \pmod{y^2}$$
$$\equiv (x+y^2)\cdot(x+1-y^2) \pmod{y^4}$$

.....

- This goes on factoring the <u>irreducible</u> f.

— Thus, Hensel lifting does not immediately solve bivariate factorization.

— Also, the <u>pseudo</u>-coprimality condition is crucial for the lift:

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

$\Rightarrow f \equiv x \cdot x \pmod{y}$

- Say, it can be lifted to
$f \equiv (x + y\,a(x,y)) \cdot (x + y\,b(x,y) \pmod{y^2}$

$\Leftrightarrow \quad x^2 + y \equiv x^2 + xy(a+b) \pmod{y^2}$
$\Leftrightarrow \quad 1 \equiv x \cdot (a+b) \pmod{y}$
$\Leftrightarrow \quad x \cdot (a(x,0) + b(x,0)) = 1$.
which is absurd!

- How do we handle this case? ($f(x,0)$ is square-full)

- Shift y: Consider $f(x,y) = x^2 + (y-1)$.

- Now, $f \equiv (x-1)(x+1) \pmod{y}$
& the lift continues!

- When should we stop the lift?

<u>Idea</u> – Suppose the lifts are $f \equiv g_k \cdot h_k \pmod{y^{2^k}}$.

- The issue is that an actual factor of f may not correspond to g_k.

(Uniquess property)

- But the Hensel lemma claims that some multiple of g_k, say $g' \equiv g_k \cdot l_k$ will be a factor of $f(x,y)$.

- So, we intend to go slightly beyond $2^k > \deg f$ & try to find a $g' \equiv g_k \cdot l_k \pmod{y^{2^k}}$ s.t. $0 < \deg_x g' < \deg_x f$ & $\deg_y g' \leq \deg_y f$.

- Such a g' (if it exists) could be found by linear algebra.
- Finally, we compute $\gcd_x(f, g')$.

- This motivates the following bivariate factoring algorithm.

<u>Input</u>: $f(x,y) \in \mathbb{F}[x,y]$ (with no univariate factors).
<u>Output</u>: A nontrivial factor of f (if one exists).
<u>Algo</u>:

(1) Preprocess f s.t. $f(x,y)$ & $f(x,0)$ are both <u>square-free</u>.
Let $\deg f =: d$ (& $\deg_x f \geq 1$).
[Also ensure $\deg_x f = \deg f(x,0)$.]

(2) Factor $f \equiv g_0(x,y) \cdot h_0(x,y) \pmod y$ s.t. g_0 is <u>monic</u> wrt x, <u>irred</u>. & $\deg_x g_0 < \deg_x f$ >0.

(3) Hensel lift k times s.t. $2^k \geqslant 2d^2$.
Let $f \equiv g_i \cdot h_i \pmod{y^{2^i}}$, $i \in [0,k]$.

(4) Solve the linear system for g' & l_k s.t.
$g' \equiv g_k \cdot l_k \pmod{y^{2^k}}$, $0 < \deg_x g' < \deg_x f$,
$\deg_y g' \leq \deg_y f$, & $(\deg_x l_k, \deg_y l_k) < (\deg_x f, 2^k)$.

(5) Output $\gcd_x(f, g')$.

Analysis:

Step 1- Say, f is square-full:

Either, a derivative, say, $\partial_x f$ is zero (in which case $f = g(x^p, y)$ for some g & $\mathrm{ch}\,\mathbb{F} =: p$).

Or, wlog $\partial_x f \neq 0$ (in which case $\gcd_x(f, \partial_x f)$ factors f).

We can use these observations to reduce the factoring of f to smaller instances.

Say, $f(x,0)$ is square-full (while f is not):

- For an $\alpha \in \mathbb{F}$, $f(x,\alpha)$ is square-full iff $\gcd_x(f(x,\alpha), \partial_x f(x,\alpha))$ is nontrivial iff $\mathrm{res}_x($ " $) = 0$.

- Recall that the resultant can be seen

nonzero
as a polynomial in α of deg $< 2d^2$.
$\Rightarrow$
If we pick $2d^2$-many α's in $\mathbb{F}$ (or in its extension), then for at least one of them $f(x,\alpha)$ is <u>square-free</u>.

$\Rightarrow$ We can use $f(x, y+\alpha)$ instead of $f(x,y)$ to factor f.
[Similar trick ensures $\deg_x f = \deg f(x,0)$.]

<u>Step 4</u> – If f is reducible then g' exists.
<u>Proof:</u>
- Since, g_0 is an irreducible factor of $f \pmod y$, it has to <u>divide</u> some suitable irreducible factor $g \in \mathbb{F}[x,y]$ of f.

$0 < \deg_x g < \deg_x f$

- Say, $f = g \cdot h$ over $\mathbb{F}$ and
$$g \equiv g_0 \cdot l_0 \pmod y.$$

- Hensel lifting (k times) gives us:
$g \equiv g'_k \cdot l'_k \pmod{y^{2^k}}$ with monic $g'_k \equiv g_0 \pmod y$.

$$\Rightarrow \quad f \equiv g_k' \, l_k' \, h \pmod{y^{2^k}}.$$

- By the uniqueness of Hensel lift, we deduce that $g_k' \equiv g_k \pmod{y^{2^k}}$.

$$\Rightarrow \quad g \equiv g_k \cdot l_k' \pmod{y^{2^k}}.$$

$\Rightarrow$ Step 4 will find a solution g' of the linear system. $\square$

<u>Step 5</u> – Using g' this step factors f.

<u>Proof:</u>

- Suppose not, then $\gcd_x(f, g') = 1$.

$\Rightarrow \exists\, u', v' \in \mathbb{F}(y)[x]$, $u'f + v'g' = 1$.

$\Rightarrow \exists\, u, v \in \mathbb{F}[x,y]$,

$$uf + vg' = \mathrm{res}_x(f, g').$$

[Use the linear algebra fact that
$A^{-1} = \mathrm{adj}(A) \cdot |A|^{-1}$.]

$\Rightarrow u\, g_k h_k + v\, g_k \ell_k \equiv res_x(f, g') \pmod{y^{2^k}}$.

$\Rightarrow g_k \cdot (u h_k + v \ell_k) \equiv res_x(f, g') \pmod{y^{2^k}}$.

- Since $0 < \deg_x g_k < \deg_x f$ & g_k is monic wrt x, while the RHS is free of x,

  the above congruence could hold only when both the sides are zero.

  $\Rightarrow res_x(f, g') \equiv 0 \pmod{y^{2^k}}$.

- But $2^k \geq 2d^2 > \deg_y res_x(f, g')$.

  $\Rightarrow res_x(f, g') = 0$.

  $\Rightarrow \gcd_x(f, g') \neq 1$, a contradiction!

$\Rightarrow$ Step 5 factors f once a g' exists.

$\square$

Theorem (Kaltofen 1982): Bivariate factoring reduces in det. poly-time to univariate polynomial factoring.

- This also generalizes to n-variates. However, for degree d, the times grows as $\binom{n+d}{d} \approx d^{O(n)}$.

Corollary: A degree d, n-variate polynomial over $\mathbb{F}_q$, can be factored in randomized $\text{poly}(d^n, \lg q)$ time.

- Now, we will focus on:

(a) Could we improve on $d^{O(n)}$ time?

(b) What about factoring over $\mathbb{Q}$?