& 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 & unique.

Proof:

- We can compute G, H s.t. $f \equiv G \cdot H \pmod{y^{2k}}$, by Hensel lemma.
- If G is not monic wrt x then correct it to $g' := g + r y^k$, where r is the remainder 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. $f(x,y) = x(x+1) + y^2$

$$
\begin{aligned}
f &\equiv x \cdot (x+1) \pmod{y} \\
&\equiv x \cdot (x+1) \pmod{y^2} \\
&\equiv (x+y^2) \cdot (x+1-y^2) \pmod{y^4} \\
&\quad \cdots\cdots
\end{aligned}
$$

- 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?

Idea — 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. $\deg_x g' < \deg_x f$ & $\deg_y g' \leq \deg_y f$.

- 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.

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

(1) Preprocess f s.t. $f(x,y)$ & $f(x,0)$ are both square-free.
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 monic wrt x, irred. & $\deg_x g_0 < \deg_x f$ > 0.

(3) Hensel lift k times s.t. $2^k > d^2$.
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.
$g' \equiv g_k \cdot \ell_k \pmod{y^{2^k}}$, $\deg_x g' < \deg_x f$,
$\deg_y g' \leq \deg_y f$, & $(\deg_x \ell_k, \deg_y \ell_k) < (\deg_x f, 2^k)$.

(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