as a nonzero polynomial in α of $\deg \le d^2$.

$\Rightarrow$

If we pick (d^2+1)-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
$$g \equiv g_0 \cdot \ell_0 \pmod y.$$

- Hensel lifting (k times) gives us:
$g \equiv g_k' \cdot \ell_k' \pmod{y^{2^k}}$ 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 $\gcd_x(f, g') = 1$.

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

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

  $$uf + vg' = res_x(f, g').$$

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

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

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

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

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

  $\Rightarrow gcd_x(f, g') \neq 1$, 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 $\mathrm{poly}(d^n, \lg q)$ time.

- Now, we will focus on:

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

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

Blackbox factoring of multivariates

- Given a polynomial $f(x, y_1, \ldots, y_n)$ of degree d.
  We want to factor f in poly(nd)-time (randomized algo.).
  Moreover, we assume that f is available only via an <u>oracle</u>. I.e. we can only evaluate f:

$$\bar{\alpha} \in \mathbb{F}^{n+1} \longrightarrow \boxed{f} \longrightarrow f(\bar{\alpha}) \in \mathbb{F} \quad .$$

- This is a powerful model as f could be "any" deg-d, $(n+1)$-variate polynomial!

- We cannot apply the Hensel lifting based factoring algo. directly, as:
  (1) it requires the "dense" representation of f,
  (2) its complexity is bad — d^n time.

Idea: • "Randomly" reduce f to a <u>3-variate</u> projection $f_a(x, t_1, t_2)$.
• <u>Factor</u> f_a in randomized poly-time.
• <u>Reconstruct</u> the <u>blackboxes</u> for the factors of f, from the factors of f_a.

- The first step has its origins from the famous "Hilbert's irreducibility theorem" (short, HIT).

<u>Theorem</u> (Hilbert 1892): Let $S \subseteq \mathbb{F}$ be a finite set of size $\geq 7d^6$, $f(x, \bar{y})$ be a monic polynomial in x with <u>total</u> degree d.

If $\partial_x f \neq 0$ and

$$\Pr_{\bar{a}, \bar{b} \in S^n} \left[f(x, a_1 t + b_1, \ldots, a_n t + b_n) \text{ is reducible} \right] \geq 7d^6/|S|$$

then f is reducible.

- Thus, reducibility in $\mathbb{F}[x, t]$ relates to $\mathbb{F}[x, \bar{y}]$.