

nonzero
as a polynomial in x of $\deg \leq d^2$.

\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 square-free.

\Rightarrow We can use $f(x, y+\alpha)$ instead of $f(x, y)$

to factor f .
[Similar trick ensures $\deg_x f = \deg f(x, 0)$.]

Step 4 - If f is reducible then g exists.

Proof:

$0 < \deg_x g < \deg_x f \rightarrow$ Since, g_0 is an irreducible factor of $f \pmod{y}$, it has to divide some suitable irreducible factor $g \in \mathbb{F}[x, y]$ of f .

• Say, $f = g \cdot h$ over \mathbb{F} and
 $g \equiv g_0 \cdot t_0 \pmod{y}$.

• Hensel lifting (k times) gives us:

$g \equiv g'_k \cdot t'_k \pmod{y^{2^k}}$ with monic $g'_k \equiv g_0 \pmod{y}$.

$$\Rightarrow f \equiv g'_k t'_k h \pmod{y^{2^k}}.$$

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

$$\Rightarrow g \equiv g_k t'_k \pmod{y^{2^k}}.$$

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

Step 5 - Using g' this step factors f .

Proof:

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

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

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

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

[Use the linear algebra fact that

$$A^{-1} = \text{adj}(A) \cdot |A|^{-1}.]$$

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

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

- 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.

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

- But $2^k > d^2 \geq \deg_y \text{res}_x(f, g')$.

$$\Rightarrow \text{res}_x(f, g') = 0.$$

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

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

□

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

- This also generalizes to n -variables. 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?

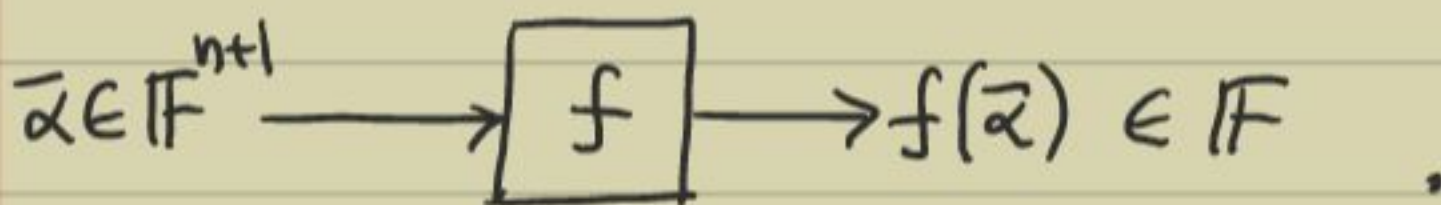
(b) What about factoring over \mathbb{Q} ?

Blackbox factoring of multivariate

- Given a polynomial $f(x, y_1, \dots, y_n)$ of degree d .

We want to factor f in $\text{poly}(nd)$ -time (randomized algo.).

Moreover, we assume that f is available only via an oracle. I.e. we can only evaluate f :



- 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 3-variate projection $f_a(x, t_1, t_2)$.
 - Factor f_a in randomized poly-time.
 - Reconstruct the blackboxes for the factors of f , from the factors of f_a .
- The first step has its origins from the famous "Hilbert's irreducibility theorem" (Shost, MIT).

Theorem (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 total degree d .

If $\partial_x f \neq 0$ and

$$\Pr_{\substack{\bar{a}, \bar{b} \in S^2 \\ |\bar{a}, \bar{b}| \geq 7d^6/|S|}} [f(x, a_1 t + b_1, \dots, a_n t + b_n) \text{ is reducible}]$$

then f is reducible.

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