- The proof of this theorem will require several lemmas.

- First, we show that given <u>any</u> $f(x,\bar{y})$, we can ensure $\deg_x f = \deg f(x,\bar{0})$. ← <u>almost</u> monic in x

- The idea is to <u>randomly</u> shift $\bar{y}$ by $\bar{a} \in \mathbb{F}^n$ to $f'(x,\bar{y}) := f(x, y_1+a_1, \ldots, y_n+a_n)$.
  It can be shown that the leading coefficient (wrt x) in f' is in $\mathbb{F}^* \bmod \langle \bar{y} \rangle$.

fraction of zeros

<u>Lemma 1</u> (DeMillo-Lipton '78, Zippel '79, Schwartz '80):
Let $F(\bar{y}) \in \mathbb{F}[\bar{y}]$ be of $\deg \le d$ & $S \subseteq \mathbb{F}$ be a finite set of size $> d$. If $F \neq 0$ then
$$\Pr_{\bar{a} \in S^n} [F(\bar{a}) = 0] \le d/|S|.$$

<u>Pf sketch</u>: • When F is a univariate, it is clear.
• For a multivariate F, use induction. $\square$

- Thus, any polynomial $f(x,\bar{y}) = \sum_{i=0}^{e} p_i(\bar{y}) \cdot x^i$ when randomly shifted to $f(x, \bar{y}+\bar{a})$ has the leading coefficient $p_e(\bar{y}+\bar{a})$ with a <u>nonzero</u> constant term $p_e(\bar{a})$, with high probability.

$$\Rightarrow \quad p_e(\bar{y}+\bar{a}) \neq 0 \mod \langle \bar{y} \rangle .$$

- From now on we assume $f(x,\bar{y})$ to be <u>almost-monic</u> in x. It is easy to deduce:

▷ If $f(x,\bar{y})$ is almost-monic in x & $g | f$, then $g(x,\bar{y})$ is also almost-monic in x.

- We will also need to handle square-fullness.

<u>Lemma 2</u>: If $\partial_x f \neq 0$ & $\Pr_{\bar{b} \in S^n} [f(x,\bar{b}) \text{ is square-full}] > \frac{d^2}{|S|}$

then f is reducible.

<u>Pf</u>: • Let $r(\bar{y}) := res_x(f, \partial_x f)$.

• We know that: $f(x,\bar{b})$ is square-full $\Rightarrow$

$r(\bar{b}) = 0$.

- Also, we have $\deg r(\bar{y}) \leq d^2$.
- $\Rightarrow$ (by Lemma 1) $\Pr_{\bar{b} \in S^n} [r(\bar{b}) = 0] \leqslant d^2/|S|$.

- As this contradicts the hypothesis, we deduce $r = 0$.

$\Rightarrow$ $\gcd_x(f, \partial_x f) \neq 1$.

$\Rightarrow$ f is reducible. $\square$

— Thus, we could assume that a random projection $f(x, \bar{a}t + \bar{b})$ is square-free whp (otherwise we already deduce that f is reducible).

— So it suffices to prove the following:

Theorem (H.I.T.): Let $f(x, \bar{y})$ be almost-monic in x, & has degree $\leq d$. If
$$\Pr_{\bar{a}, \bar{b} \in S^n} [\, f(x, \bar{a}t + \bar{b}) \text{ is reducible, sq-free} \,] \geqslant \frac{7d^6}{|S|}$$
then f is reducible.

Pf: • Let $f(x, \bar{a}t+\bar{b})$ be reducible & sq-free.

• For simplicity we work with $\bar{b}=0$.

• Let $f(x,\bar{a}t)$ factor as:

$$f(x,\bar{a}t) \equiv g_0(x) \cdot h_0(x) \pmod t.$$

[$\deg_x f = \deg f(x,0)$, g_0 is an irred. proper factor coprime to h_0]

• Which on Hensel lifting gives:

$$f(x,\bar{a}t) \equiv g_{k,\bar{a}}(x,t) \cdot h_{k,\bar{a}}(x,t) \pmod{t^{2^k}}. \quad \text{---- (i)}$$

• We could take another Hensel lifting route:

$$f(x,\bar{y}t) \equiv g_0(x) \cdot h_0(x) \mod \langle \bar{y} \rangle.$$

$$\vdots$$

deg wrt t is $< 2^k$ →

$$f(x,\bar{y}t) \equiv g'_k(x,t,\bar{y}) \cdot h'_k(x,t,\bar{y}) \mod \langle \bar{y} \rangle^{2^k}.$$

$$\Rightarrow \quad \text{''} \quad \equiv \quad \text{''} \quad \pmod{t^{2^k}}. \quad \text{---- (ii)}$$

• By the factorizations (i) & (ii) of $f(x,\bar{a}t)$, and the uniqueness of Hensel lifting ($\because f$ is almost-monic in x), we conclude:

g'_k is independent of $\bar{a}$! →

$$g_{k,\bar{a}}(x,t) = g'_k(x,t,\bar{a}) \pmod{t^{2^k}}.$$

- Thus, $g_k'(x,t,\bar{y})$ is a <u>potential</u> factor of $f(x,\bar{y}t)$. But, we need to do some more work as in the case of "bivariate factoring".

<u>Claim 1:</u> By the prob. hypothesis of the thm., there are
$d^2 < 2^k \leq 2d^2 \to$ polynomials $g(x,t,\bar{y})$ & $\ell_k(x,t,\bar{y})$ satisfying a nontrivial eqn. $g \equiv g_k' \cdot \ell_k \pmod{t^{2^k}}$,
with $\deg_x g < \deg_x f(x,\bar{y}t)$, $\deg_t g \leq d$,
$\sum_{i=1}^{n} \deg_{y_i} g \leq 6d^5$.

<u>Pf:</u> • We have a <u>good</u> fraction of $\bar{a}$ in S^n s.t. $f(\bar{x},\bar{a}t)$ has a liftable factorization; implying the existence of $g_{\bar{a}}, \ell_{k,\bar{a}}$ s.t.

$\deg_t \leq d \to$ $g_{\bar{a}}(x,t) \equiv g_k'(x,t,\bar{a}) \cdot \ell_{k,\bar{a}}(x,t) \bmod t^{2^k}$.

- Here, #unknowns $< d \cdot d + d \cdot 2^k \leq (d^2 + 2d^3) \leq 3d^3$.
- Now consider the homog. lr. system
$$g(x,t,\bar{y}) \equiv g_k'(x,t,\bar{y}) \cdot \ell_k(x,t,\bar{y}) \bmod t^{2^k}.$$
viewing g, g_k', ℓ_k as bivariates over $\mathbb{F}(\bar{y})$.