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:

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

- 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

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

then f is reducible.

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

- 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

$$\Pr_{\bar{a} \in S^n} [F(\bar{a}) = 0] \le d/|S| .$$

[I.e. nonzeros are dense in S^n]

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

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

- We will also need to handle square-fullness.

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

then f is reducible.

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

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

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

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

- 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

$$\Pr_{\bar{a}, \bar{b} \in S^n} \left[\begin{array}{l} f(x, \bar{a}t + \bar{b}) \text{ is reducible } \& \\ f(x, \bar{b}) \text{ is sq-free} \end{array} \right] \geq \frac{7d^6}{|S|}$$

then f is reducible.

Idea — We want to move from $\bar{a}$ to formal $\bar{y}$.

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 $< 2^k$ → $f(x, \bar{y}t) \equiv g_k'(x,t,\bar{y}) \cdot h_k'(x,t,\bar{y}) \mod \langle \bar{y} \rangle^{2^k}$.

$\Rightarrow$ " $\equiv$ " $\pmod{t^{2^k}}$.

[$\because t$ is merely a $\deg_{\bar{y}}$-counter] ---- (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 $\bar{a}$! → $g_{k,\bar{a}}(x,t) = \underline{g_k'}(x,t,\bar{a}) \pmod{t^{2^k}}$.

g_k' becomes the common thread

- 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 $\deg_x g < \deg_x f(x,\bar{y}t)$, $\deg_t g \leq d$,

$\deg_{\bar{y}} g := \sum_{i=1}^{n} \deg_{y_i} g \leq 6d^5$.

<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 $\mathbb{F}(\bar{y})$.

- Obviously, the #unknowns $\underline{m}$ is still $< 3d^3$.
- If it has $\underline{\text{no}}$ solution, then the corresponding $m \times m$ matrix M (with entries as coefficients of g_k) has a $\underline{\text{nonzero}}$ determinant $D(\bar{y})$.

$$\Rightarrow \deg D(\bar{y}) < m \cdot 2^k \leq 3d^3 \cdot 2d^2 = 6d^5.$$

$$\Rightarrow \Pr_{\bar{a} \in S^n}[D(\bar{a}) = 0] \leq 6d^5 / |S|.$$

- On the other hand, by the hypothesis, the system has a solution for "many" $\bar{y} = \bar{a} \in S^n$, in which cases $D(\bar{a}) = 0$.

This contradiction implies $D(\bar{y}) = 0$.

$$\Rightarrow g(x, t, \bar{y}) \ \& \ l_k \text{ do exist!}$$

- The $\sum_i \deg_{y_i} g \leq \deg |M|$ follows from the Cramer's rule of solving linear system of equations. $\square$

- Finally, we want to use $g(x, t, \bar{y})$ to factor $f(x, \bar{y}t)$.

actually, $t=1$ suffices here

- Consider $r(t,\bar{y}) := res_x\left(f(x,\bar{y}t),\, g(x,t,\bar{y})\right)$.

  $\Rightarrow \deg r \leq d\cdot(d+d+6d^5) < 7d^6$ [$\because d \geq 2$]

  [However, $\deg_t r \leq d\cdot d = d^2 < 2^k$.]

- On the other hand, we know from "bivariate factoring" proof & the construction of g that $r(t,\bar{a})=0$, for a "good" fraction of $\bar{a}\in S^n$.

  $\Rightarrow r(t,\bar{y}) = 0$.

  $\Rightarrow \gcd_x\left(f(x,\bar{y}t),\, g(x,t,\bar{y})\right) \neq 1$.

  $\Rightarrow f$ is reducible.

- This proves HIT! $\square$

Blackbox factoring algorithm

Input: Oracle to $f(x,\bar{y}) \in \mathbb{F}[x,\bar{y}]$ of deg d & $S \subseteq \mathbb{F}$ s.t. $|S| > 7d^7$.

f is almost-monic in x & $\partial_x f \neq 0$.

Output: Blackboxes to the factors of f.

Algo: 1) We compute the number of factors by:

1.1) Pick $\bar{a}, \bar{b} \in S^n$ randomly.

1.2) Factor $f_{\bar{a},\bar{b}}(x,t) := f(x, \bar{a}t+\bar{b})$.

Let $\{\tilde{f}_i(x,t) \mid i \in [\ell]\}$ be the irreducible factors.

[$\triangleright$ Whp ℓ is the number of factors of $f(x,\bar{y})$.

Pf: Let $f_i(x,\bar{y})$, $i \in [\ell']$, be the actual factors. These are all almost-monic irreducibles.

By H.I.T.: $f_i(x, \bar{a}t+\bar{b})$ is reducible with prob. $< 7d^6/|S|$.

$\Rightarrow \Pr[\exists i,\ f_i(x,\bar{a}t+\bar{b}) \text{ reduces}] < 7d^7/|S|$. $\square$]

2) Assuming that $\tilde{f}_i(x,t)$ is the projection of an actual factor, i.e. $\tilde{f}_i = f_i(x, \bar{a}t+\bar{b})$, we want to compute the value $f_i(\alpha,\bar{\beta})$ for any given $(\alpha,\bar{\beta}) \in \mathbb{F}^{n+1}$.

For this we define a trivariate that "contains" both the <u>projections of f</u> to the <u>line</u> $\bar{a}t+\bar{b}$ & the <u>point</u> $(\alpha,\bar{\beta})$:

$$g(x,t_1,t_2) := f(x, \bar{a}t_1+\bar{b}+(\bar{\beta}-\bar{b})t_2).$$

$\triangleright$ $g(x,t,0) = f(x,\bar{a}t+\bar{b})$ & $g(\alpha,0,1) = f(\alpha,\bar{\beta})$.

3) Now we factor g to compute $f_i(\alpha, \bar{\beta})$:

3.1) Using 3-variate factoring, find the irreducible factors $\{g_j(x, t_1, t_2) \mid j \in [\ell]\}$ whp.

3.2) Find the index j s.t. $\tilde{f}_i(x,t) = g_j(x,t,0)$.

3.3) Output $g_j(\alpha, 0, 1)$.

[Whp we will get the factors g_j that exactly are projections like $f_i(x, \bar{a}t_1 + \bar{b} + (\bar{\beta} - \bar{b})t_2)$.]

<u>Theorem</u> (Kaltofen & Trager, 1990): Given $f(x, \bar{y})$, as a blackbox, one can factorize f (as blackboxes) in randomized poly(n,d) time (assuming that univariate factoring can be done).