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)-many field operations (randomized algorithm). Moreover, f is available only via oracle, i.e. we can 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, $(n+1)$-var. poly.!

- Cannot apply "Hensel lifting" based algorithm directly because:
  1) it requires dense representation of $f(x, \bar{y})$.
  2) its complexity is d^n — exp. higher than dn.

Idea:
- Randomly reduce f to a 3-variate projection $f_a(x, t_1, t_2)$. [Ex: Interpolate f for small n.]
- 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 in the famous: Hilbert's Irreducibility Theorem (HIT).

Theorem (Hilbert 1892): Let $S \subseteq \mathbb{F}$ be a finite subset large enough ; $f(x, \bar{y})$ is a monic polynomial in x with total degree d.

If $\partial_x f \neq 0$ & f is irreducible then:

$$\Pr_{\bar{a}, \bar{b} \in S^n} [\, f(x, a_1 t_1 + b_1, \ldots, a_n t_1 + b_n) \text{ is reducible} \,] \leq (7d^6 + 2d^2 + d)/|S| .$$

[false for univariate projection]

– To prove this theorem, we need some lemmas.

<u>Lemma 1:</u> (Polynomial Identity Lemma): Let $F(\bar{y}) \in \mathbb{F}[\bar{y}]$ be of degree d & $S \subseteq \mathbb{F}$ is a finite subset of size $> d$.

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

<u>Pf. Sketch:</u>
- For $n=1$, it is clear.
- For $n>1$, use induction on n. $\square$

$\Rightarrow$ Nonzeros of f are <u>dense</u> in S^n.

- **Defn:** $f(x,\bar{y})$ is called <u>almost-monic</u> in x, if $\deg_x f = \deg f(x,\bar{0})$.

▷ $f(x, \bar{y}+\bar{\alpha})$ is <u>whp</u> almost-monic, for $\bar{\alpha} \in_R S^n$.

Pf:

- Say, $f(x,\bar{y}) =: \sum_{i=0}^{e} p_i(\bar{y}) \cdot x^i$ with $p_e(\bar{y}) \neq 0$.
- By PIL, $\Pr_{\bar{a}\in S^n}[p_e(\bar{a})=0] \leqslant d/|S|$.

$\Rightarrow$ whp $f(x,\bar{y}+\bar{a})$ is almost-monic $\square$

▷ Factors of almost-monic poly. are almost-monic.

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

Pf: • Square-fullness relates to the discriminant:

$r(\bar{y}) := \mathrm{res}_x(f, \partial_x f) \neq 0$. $[\gcd_x(f, \partial_x f) = 1.]$

▷ $f(x,\bar{b})$ is square-full $\Longrightarrow r(\bar{b}) = 0$.

• Note that $r(\bar{y})$ is nonzero & $\deg r < 2d^2$.

$\Rightarrow$ (by PIL) $\Pr_{\bar{b}\in S^n}[\, r(\bar{b}) = 0 \,] < 2d^2/|S|$.

$\Rightarrow \Pr_{\bar{b}\in S^n}[\, f(x,\bar{b}) \text{ is sq-full} \,] < 2d^2/|S|$. $\square$

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

- So, it suffices to prove the following:

Theorem (H.I.T.): Let $f(x,\bar{y})$ be almost-monic & irreducible. Then, $\Pr_{\bar{a},\bar{b}\in S^n}[\, f(x,\bar{a}t+\bar{b}) \text{ is reducible } \& \ f(x,\bar{b}) \text{ is sq. free}] < 7d^6/|S|$.

Pf. idea: We want to move from fixed $\bar{a}$ to the formal $\bar{y}$. ($\bar{a}t+\bar{b}$ to $\bar{y}\cdot t+\bar{b}$)

- For notation simplicity we assume wlog $\bar{b}=0$.

Proof: • Assume $f(x, \bar{a}t)$ is reducible & sq-free, & for "most" $\bar{a} \in S^n$

• Hensel lift mod $\langle t \rangle$-powers:

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

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

$$\Rightarrow \quad f(x, \bar{a}t) \equiv \underline{g_{k,\bar{a}}(x)} \cdot h_{k,\bar{a}}(x) \mod \langle t \rangle^{2^k} \quad \text{---} (i)$$

• Hensel lift mod $\langle \bar{y} \rangle$-powers:

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

$$\vdots$$

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

$$\Rightarrow \quad f(x, \bar{y} \cdot t) \equiv \underline{g_k'} \cdot h_k' \mod \langle t \rangle^{2^k} . \quad \text{---} (ii)$$

- By Factorizations (i) & (ii) of $f(x, \bar{a}\cdot t)$, & the uniqueness of Hensel lifting ($\because f$ is almost-monic) we conclude: $g_{k,\bar{a}}(x,t) = g'_k(x,t,\bar{a}) \bmod \langle t\rangle^{2^k}$.

- Thus, $g'_k(x,t,\bar{y})$ is a potential factor of $f(x,\bar{y}\cdot t)$.
- So, consider a linear system, as done in the case of "bivariate factoring".

Claim 1: Whp, $\exists\, g, \ell_k \in \mathbb{F}[x,t,\bar{y}]$ s.t.

$$g \equiv g'_k \cdot \ell_k \bmod \langle t\rangle^{2^k} \text{ with } \deg_x g < \deg_x f(x,\bar{y}\cdot t),\ \deg_t g \leq d,$$

$$d_{\bar{y}} := \sum_{i\in[n]} \deg_{y_i} g \leqslant 6d^5. \quad [\text{Pick } d^2 < 2^k \leq 2d^2.]$$

Proof: • We have a good fraction of $\bar{a} \in S^n$ s.t. $f(x, \bar{a}\cdot t)$ has a liftable factorization.

$\Rightarrow \exists\, g_{\bar{a}}, \ell_{k,\bar{a}}$ s.t. $g_{\bar{a}}(x,t) \equiv g_k'(x,t,\bar{a}) \cdot \ell_{k,\bar{a}}(x,t) \mod \langle t \rangle^{2^k}$.

• On the other hand, consider the equation over $\mathbb{F}(\bar{y})$:

$$g(x,t,\bar{y}) \equiv g_k' \cdot \ell_k \mod \langle t \rangle^{2^k}. \quad \text{---(iii)}$$

Idea: This linear system should have a solution, since for most $\bar{y} \leftarrow \bar{a} \in S^n$, the system has a solution.

▷ # unknowns (in $\mathbb{F}(\bar{y})$) $m < \underbrace{d \cdot d}_{g} + \underbrace{d \cdot 2^k}_{\ell_k}$

$\leq d^2 + d \cdot 2d^2 \leq 3d^3$.

– Compare (x,t)-monomials both sides, to get the constraints.

— If eqn.(iii) has no nonzero solution, then the corresponding $m \times m$ matrix M (with entries as coeffs. of g_k') has a nonzero determinant $D(\bar{y}) \neq 0$.

$\Rightarrow$ $\deg D \leq m \cdot 2^k \leq 3d^3 \cdot 2d^2 = 6d^5$.

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

$\Rightarrow$ For "most" $\bar{y} \leftarrow \bar{a}$ the system has no nonzero solution. $\Rightarrow$ $\lightning$.

$\Rightarrow$ g & l_k exist.

- $\sum_{i \in [n]} \deg_{y_i} g \leq \deg \det(M) = \deg D(\bar{y}) \leq 6d^5$.

(Cramer's rule)

$\square$

- Finally, we want to use $g(x,t,\bar{y})$ to factor $f(x,\bar{y}\cdot t)$.
- Idea: Consider $\gcd_x(f(x,\bar{y}t), g(x,t,\bar{y}))$.
- Consider $r(t,\bar{y}) := \mathrm{res}_x($ " , " $)$.

  $\Rightarrow \deg r \le d\cdot(d+d+6d^5) < 7d^6$. $(\because d \ge 2)$.

  While $\deg_t r \le d\cdot d < 2^k$.

• On the other hand, for most $\bar{a}\in S^n$, $r(t,\bar{a})=0$.

  [using "bivariate-factoring" proof-technique]

  $\Longrightarrow$ (by PIL) $r(t,\bar{y})=0$ [requires: $\deg_t r < 2^k$]

  $\Rightarrow \gcd_x(f(x,\bar{y}t), g(x,t,\bar{y})) \ne 1 \Rightarrow f$ is reducible.

• Proves H.I.T.! $\square$

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

Output: Blackboxes to irreducible factors of f (assuming univariate factoring over $\mathbb{F}$).

Idea: To compute $f_i(\alpha,\bar{\beta})$, for factor f_i, project to 3-variate & factor f (invoking H.I.T.).

Algo: 1) Compute #factors by:

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

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

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

2) Assuming $\tilde{f}_i$ is the projection of an actual factor of f, i.e. $\tilde{f}_i = f_i(x, \bar{a}\cdot t + \bar{b})$:

we want the value $f_i(\alpha, \bar{\beta})$, for $\alpha, \bar{\beta} \in \mathbb{F}^{n+1}$.

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

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

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

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

3.1) Using 3-var. 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 $g_j(\alpha,0,1)$ [$= f_i(\alpha,\bar{\beta})$.]

Correctness: ▷ Whp ℓ is the # irreducible factors of $f(x,\bar{y})$. [Pf: Follows from H.I.T. with error-probability $< d \cdot 7d^6/|S| = 7d^7/|S|$.]

▷ Whp $g_j(x,t_1,t_2)$ is exactly like some $f_i(x, \bar{a}t_1 + \bar{b} + (\bar{\beta}-\bar{b})t_2)$, for irreducible factor f_i of f.

Theorem (Kaltofen & Trager, 1990): Given $f(x, \bar{y})$, as a blackbox, one can factorize f (as blackboxes) in randomized poly(n, d)-time (assuming 1-var. factoring).

$\Rightarrow$ Irreducibility testing of blackboxes.

$\Rightarrow$ Small circuits have factors that are again small circuits!

$\Rightarrow$ Algebraic circuit classes are closed under factors!