- 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 $D(\bar{y}) = 0$.

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

- 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. $< 7d^6/|S|$.

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

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 projections of f to the line $\bar{a}t+\bar{b}$ & the point $(\alpha,\bar{\beta})$:

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

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

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 $f_i(x, \bar{a}t_1 + \bar{c} + (\bar{\beta} - \bar{c})t_2)$.]

<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).