

Sparse Polynomial Interpolation

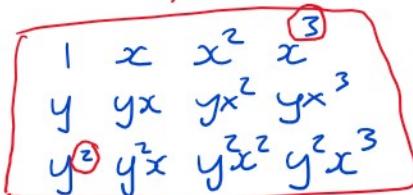
Let $g \in R[x_1, \dots, x_n]$, R is a ring.

Let $\#g$ denote the number of non-zero terms.

Suppose $t = \#g$ and $d_i = \deg(g, x_i)$.

Then $t \leq M = \prod_{i=1}^n (1+d_i)$.

Ex 1. $g \in \mathbb{Z}[x_1, y]$
 $\underline{d_1=3} \quad \underline{d_2=2}$

3 4

 $M = 3 \cdot 4 = 12$.

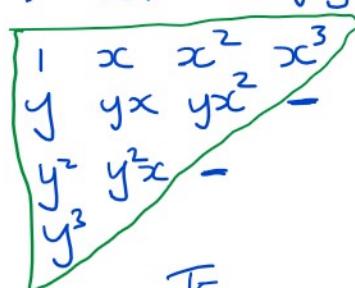
We say g is sparse if $t = \#g \ll M$? $t \leq \sqrt{M}$?

Ex 2. $g = 2x_1^3 + 3x_1x_2 + 5x_3^3 + 6x_1x_2x_4 + 7x_1x_2x_3 - 1$.
 $\underline{t=6} \quad M = 4 \cdot 2 \cdot 4 \cdot 3 = 8 \cdot 12 = 96 \quad \lceil \sqrt{M} \rceil = 10$.

Alternative (total degree). Let $d = \deg(g)$. $\#g \leq \binom{n+d}{d} = M$

Ex. $\underline{n=2} \quad \underline{d=3}$

$$M = \binom{2+3}{3} = \binom{5}{3} \\ = \frac{5!}{3!2!} = \frac{5 \cdot 4 \cdot 3!}{3! \cdot 2} \\ = 10.$$



T5

Ex 4. $g = \det(\begin{bmatrix} x & y & z & v & w \\ y & x & y & z & v \\ z & y & x & z & z \\ v & z & y & x & y \\ w & v & z & y & x \end{bmatrix})$ $\#g = 35$
 $n=5$
 $d=5$
 $M = \binom{5+5}{5} = 252$.
 $\sqrt{M} \approx 16$.

Motivation. We seek algorithms with complexity polynomial in n, t, d . Not $\binom{n+d}{d}$.

Let $a, b \in \mathbb{Z}[x_1, \dots, x_n]$, $g = \gcd(a, b)$, $a = g\bar{a}$, $b = g\bar{b}$,
 $\deg(g, x_i) = \underline{d_i}$, $t = \#g$.

\sim we use $\langle L \rangle = \langle g_1, \dots, g_t \rangle$, $g = \text{gcd}(g_1, \dots, g_t)$, $\deg(g_i) = d_i$, $t = \#g$.

Brown (1971) PGCD requires $\geq (d+1)^{\frac{n-1}{n}}$ points
 $\Rightarrow (d+1)^{n-1}$ EA. $\Rightarrow O(d^{n+1})$ ops. in \mathbb{Z}_p .

Zippel (1979) PGCD requires $\leq (d+1)(t+1)(n-1) \Rightarrow O(ndt)$ ops.
 + solve $(n-1)$ of linear systems of size $t \times t$
 $\Rightarrow O(t^3)$ ops + $O(t^2)$ space.

\rightarrow Zippel (1990) \downarrow $O(t^2)$ ops + \downarrow $O(t)$ space.

Zippel's Algorithm

PGCD($a(x,y,z)$, $b(x,y,z)$, $p=7$) Let $g = \text{gcd}(a, b)$.

Suppose $g = 1 \cdot x^4 + 3yx^2 + 5zyx^2 + zy^4z - 1$.

Write $g = 1 \cdot x^4 + (3+5z)yx^2 + (2z)y^4 - 1$. in $\mathbb{Z}_p[z][x,y]$

Observe $\deg(g, z) = 1 \Rightarrow z$ images to interpolate z .

Write $g = \sum_{i=1}^s a_i(z) \cdot M_i(x,y)$ where M_i are monomials.

① Pick $z = \alpha = 1$ at random from \mathbb{Z}_p . $p=7$

Call PGCD($a(x,y,1)$, $b(x,y,1)$) recursively.

It returns $g(x,y,1) = 1 \cdot x^4 + 1 \cdot yx^2 + zy^4 - 1 \in \mathbb{Z}_p[x,y]$
 \uparrow_{monic} .

Zippel's assumption. If p is large and α is chosen randomly from \mathbb{Z}_p Then

(i) $\text{gcd}(\bar{a}(x,y,\alpha), \bar{b}(x,y,\alpha)) = 1$ w.h.p.

(ii) $a_i(\alpha) \neq 0$ for $1 \leq i \leq s$ w.h.p.

\Rightarrow The monomials in $g(x,y,0)$ are $x^4, yx^2, y^4, 1$.

Def. α loses terms if assumption (ii) is false.

$a_i(z) = 1, 3+5z, 2z, -1$. $\xrightarrow{\alpha=0} 3+5z=0 \text{ in } \mathbb{Z}_7$
 $\alpha=5$.

$$\text{Prob}[\alpha \text{ loses terms}] \leq \frac{\deg(g, z)}{p} \cdot S$$

$a_i(z) \in \mathbb{Z}_p[z]$

- ② Pick $z=2$ at random. SGCD.
 Determine $g(x, y, z) = 1 \cdot x^4 + 6yx^2 + 4y^4 - 1$. How?

Pick $y=1$ at random and compute

$$g(a(x, 1, z), b(x, 1, z)) = 1 \cdot x^4 + 6x^2 + 3.$$

Apply (ii) let $gf(x, y, z) = 1 \cdot x^4 + c_1 x^2 y + c_2 y^4 + c_3 \cdot 1$ from

$$\text{We have } \underbrace{gf(x, 1, z)}_{=} = 1 \cdot x^4 + c_1 x^2 + (c_2 + c_3) \cdot x^0 = 1 \cdot x^4 + 6x^2 + 3.$$

$$[\text{EQ. coeffs in } x^i]: c_1 = 6, c_2 + c_3 = 3.$$

Pick $y=0$ at random and compute

$$g(a(x, 0, z), b(x, 0, z)) = 1 \cdot x^4 - 1.$$

$$gf(x, 0, z) = 1 \cdot x^4 + c_3 = 1 \cdot x^4 - 1 \Rightarrow c_3 = +6.$$

$$c_2 + c_3 = 3 \Rightarrow c_2 + 6 = 3 \Rightarrow c_2 = +4 \text{ mod 7.}$$

$$\text{Hence } g(x, y, z) = 1 \cdot x^4 + 6x^2y + 4y^4 + 6.$$

Ques? To interpolate $g(x, y, z=2)$ we needed 2 values
 for y ($y=1, y=0$) instead of $\deg(g, y) + 1 = 5$.

Coot: Depends on maximum of the #terms in the
 coefficients of x^i in g .

Note: If gf is wrong (α loses terms) we discover
 this by doing one more value for y and w.h.p.
 The linear system will be inconsistent.

- ③ Dense interpolate z . In PGCD ($p=7$). we have

$$\text{PGCD } g(x, y, 1) = 1 \cdot x^4 + \cancel{1}y \cdot x^2 + \cancel{2}y^4 \cancel{-1}.$$

$$\text{SGCD } g(x, y, 2) = 1 \cdot x^4 + \cancel{b}y \cdot x^2 + \cancel{4}y^4 \cancel{-1}.$$

$$\text{SGCD } g(x, y, z) = \underbrace{1 \cdot x^4 + 4y^2z^2}_{\text{DENSE.}} + \underbrace{(3+5z)y^2x^2 + z^2y^4 - 1}_{\text{DENSE.}}$$

$$\text{Interpolate: } g(x, y, z) = 1 \cdot x^4 + (3+5z)y^2x^2 + z^2y^4 - 1$$

What if we don't know $\deg(g, z)$?

Method (A) We "discover" $\deg(g, z)$ w.h.p. by using random evaluation points for z and stopping when the degree a , the interpolated result does not change.

$$\text{SGCD } g(x, y, z) = 1 \cdot x^4 + 4 \cdot y^2z^2 + 6y^4 - 1.$$

$$g(x, y, z) = 1 \cdot x^4 + (3+5z)y^2x^2 + (2z)y^4 - 1.$$

STOP $\Rightarrow 3$ images $\deg(g, z) + z$ images.

Method (B) Apply Lemma 7.3.

Pick $\alpha, \beta \in \mathbb{Z}_p$ at random. $\mathbb{Z}_p[x]$

$$\underline{\deg(g, z)} \leq \deg(\gcd(a(x, \alpha, \beta), b(x, \alpha, \beta)))$$

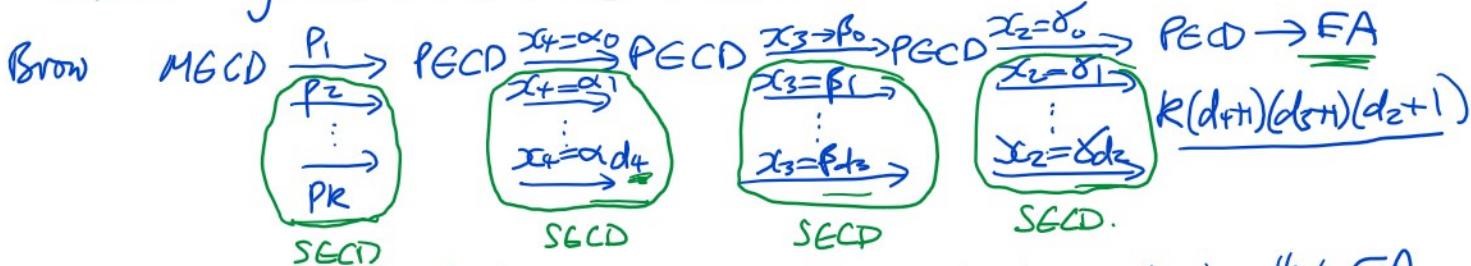
provided $\text{coeff}(a, x)(\alpha, \beta) \neq 0$.

Cont: let $g = 1 \cdot x_1^{d_1} + \sum_{i=0}^{d-1} b_i(x_2, \dots, x_n) \cdot x_1^i$ and $t = \max_{i \geq 0} \# b_i$

The linear systems are of size $(t+1) \times (t+1) \Rightarrow O(t^3)$ time
+ $O(t^2)$ space.

Zippel [1990] evaluates $a(x, y=\alpha^i, z=z)$, $b(x, y=\alpha^i, z=z)$
for $i=0, 1, \dots, t$ so that the linear systems can be
solved in $O(t^2)$ time + $O(t)$ space.

Suppose $g = x_1^{d_1} + x_2^{d_2} + x_3^{d_3} + x_4^{d_4} + 1234567890123$.



$(k-1) + d_4 + d_3 + d_2$ calls to SGCD. $\leq t+1$ calls to FA.