Zippel's Sparse GCD Algorithm

October 13, 2021 11:10 PM

Sparse Polynomial Interpolation

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

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

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

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

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

$$\begin{array}{cc} & 4 \\ 3 & \boxed{\begin{array}{cccc} 1 & x & x^2 & x^3 \\ y & yx & yx^2 & yx^3 \\ y^2 & y^2x & y^2x^2 & y^2x^3 \end{array}} \end{array} \qquad M = 3 \cdot 4 = 12.$$

We say g is *sparse* if $t = \#g \ll M$. ? $\quad t \le \sqrt{M}$. ?

Ex 2. $g = 2x_1^3 + 3x_1x_2 + 5x_3^3 + 6x_1x_4^2 + 7x_1x_2x_4 - 1.$

$t = 6 \qquad M = 4 \cdot 2 \cdot 4 \cdot 3 = 8 \cdot 12 = 96 \qquad \lceil \sqrt{M} \rceil = 10.$

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

Ex. $n = 2 \quad d = 3$

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

$$\begin{array}{cccc} 1 & x & x^2 & x^3 \\ y & yx & yx^2 & \\ y^2 & y^2x & & \\ y^3 & & & \end{array}$$

Ex 4. $$g = \det\left(\overset{T_5}{\begin{bmatrix} x & y & z & v & w \\ y & x & y & z & v \\ z & y & x & y & z \\ v & z & y & x & y \\ w & v & z & y & x \end{bmatrix}} \right)$$

$\#g = 35$

$n = 5$

$d = 5$

$M = \binom{5+5}{5} = 252.$

$\sqrt{M} \approx 16.$

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

Let $a, b \in \mathbb{Z}[x_1, \ldots, x_n]$, $g = \gcd(a, b)$, $a = g\,\bar{a}$, $b = g \cdot \bar{b}$,

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

Let $a,b \in \mathbb{Z}[x_1,\dots,x_n]$, $g = \gcd(a,b)$, $\deg a$, $\deg b$,

$\deg(g, x_i) = \underline{d}$, $t = \#g$.

Brown (1971) $\underline{P}$GCD requires $\geq (d+1)^{n-1}$ points

$\Rightarrow (d+1)^{n-1}$ E.A. $\Rightarrow O(d^{n+1})$ ops. in $\mathbb{Z}_p$.

Zippel (1979) PGCD requires $\leq (d+1)(t+1)(n-1) \Rightarrow O(ndt)$ ops.

$+$ solve $(n-1)d$ linear systems of size $t \times t$

$\Rightarrow O(t^3)$ ops $+$ $\underline{O(t^2)}$ space.

$\downarrow \qquad\qquad \downarrow$

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

Zippel's Algorithm

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

Suppose $g = 1 \cdot x^4 + 3\underline{y}x^2 + 5z\underline{y}x^2 + 2y^4z - 1$.

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

Observe $\deg(g,z) = 1 \Rightarrow 2$ 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 $g(x,y,1) = 1 \cdot x^4 + 1 \cdot yx^2 + 2y^4 - 1 \cdot 1 \in \mathbb{Z}_p[x,y]$

$\uparrow$ monic.

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

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

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

$\Rightarrow$ The monomials in $g(x,y,\cdot)$ 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. $\quad \alpha = 0 \qquad 3+5z=0$ in $\mathbb{Z}_7$

$\alpha = 5$.

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

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

(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

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

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

We have $gf(x,1,2) = 1\cdot x^4 + c_1 x^2 + (c_2+c_3)\cdot x^0 = 1\cdot x^4 + 6x^3 + 3.$

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

Pick $y=0$ at random and compute

$$g(a(x,0,2), b(x,0,2)) = 1\cdot x^4 - 1.$$

$$gf(x,0,2) = 1\cdot x^4 + c_3 = 1\cdot x^4 - 1. \Rightarrow c_3 = +6.$$

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

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

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

Cost: 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

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

SGCD $g(x,y,2) = 1\cdot x^4 + 6yx^2 + 4y^4 \; -1.$

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

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

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 of the interpolated result does not change.

SGCD $g(x,y,3) = 1\cdot x^4 + 4\cdot yx^2 + 6y^4 - 1$.

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

STOP $\Rightarrow$ 3 images $\deg(g,z)+2$ images.

Method (B) Apply Lemma 7.3.

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

$$\underline{\deg(g,z)} \leq \deg(\underset{\in\, \mathbb{Z}_p[x]}{\gcd(a(x,\alpha,\beta), b(x,\alpha,\beta))})$$

provided $\mathrm{lcoeff}(a,x)(\alpha,\beta) \neq 0$.

Cost: 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 $t = \max_{i=0}^{d-1} \# b_i$

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

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

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

Brown MGCD $\xrightarrow{p_1, p_2, \dots, p_k}$ PGCD $\xrightarrow{x_4=\alpha_0, x_4=\alpha_1, \dots, x_4=\alpha_{d_4}}$ PGCD $\xrightarrow{x_3=\beta_0, x_3=\beta_1, \dots, x_3=\beta_{d_3}}$ PGCD $\xrightarrow{x_2=\gamma_0, x_2=\gamma_1, \dots, x_2=\gamma_{d_2}}$ PGCD $\rightarrow$ EA

SGCD SGCD SGCD SGCD.

$\underline{k(d_4+1)(d_3+1)(d_2+1)}$

$(k-1)+d_4+d_3+d_2$ calls to SGCD. $\leq \underline{t+1}$ calls to EA.