Solving Transposed Vandermonde Systems

November 23, 2023 7:07 PM

Zippel 1990.

In Zippel's algorithm we need to solve linear systems of size $t \times t$ in general.

We had

$$f(\beta_i, x_2, x_3) = a_1 \cdot x_3^2 + a_2 x_2^2 x_3 + a_3 x_2.$$

and we chose (for $\beta_1 = 2$) $x_2, x_3 = (1,3), (2,1), (3,0)$. arbitrarily to get a 3×3 system.

Suppose

$$f(x,y) = \sum_{j=1}^{t} a_j \underbrace{M_j(x,y)}_{\text{monomials}} \quad \text{where } a_j \text{ are unknown.}$$

Pick $\alpha_1 \neq \alpha_2 \in \mathbb{Z}_p$ at random and use

$$(\alpha_1^j, \alpha_2^j) \text{ for } j = 0, 1, \ldots, t-1.$$

Compute

$$b_i = f(\alpha_1^j, \alpha_2^j) \text{ for } 0 \leq j < t.$$

Let $\beta_j = M_j(\alpha_1, \alpha_2)$.

$$M_j(\alpha_1^i, \alpha_2^i) = (\alpha_1^i)^{e_1} \cdot (\alpha_2^i)^{e_2} = (\alpha_1^{e_1})^i \cdot (\alpha_2^{e_2})^i = M_j(\alpha_1, \alpha_2)^i = \beta_j^i$$

$$\Rightarrow \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \cdots & \beta_t \\ \vdots & & & \\ \beta_1^{t-1} & \beta_2^{t-1} & \cdots & \beta_t^{t-1} \end{bmatrix} \overset{?}{\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_t \end{bmatrix}} = \begin{bmatrix} f(1,1) \\ f(\alpha_1, \alpha_2) \\ \vdots \\ f(\alpha_1^{t-1}, \alpha_2^{t-1}) \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_t \end{bmatrix}$$

$$A \qquad a = b.$$

A^T is a Vandermonde matrix.

So $\det(A) \neq 0 \iff \beta_i \neq \beta_j$.

$$\text{Let } A^{-1} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1t} \\ a_{21} & a_{22} & \cdots & a_{2t} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ a_{t1} & a_{t2} & \cdots & a_{tt} \end{bmatrix} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \cdots & \beta_t \\ \vdots & & & \\ \vdots & & & \\ \beta_1^{t-1} & \beta_2^{t-1} & \cdots & \beta_t^{t-1} \end{bmatrix} = \begin{bmatrix} \overset{1}{P_1(\beta_1)} & \overset{0}{P_1(\beta_2)} & \cdots & \overset{0}{P_1(\beta_t)} \\ \underset{0}{P_2(\beta_1)} & \underset{1}{P_2(\beta_2)} & \cdots & \underset{0}{P_2(\beta_t)} \\ \vdots & & & \\ \overset{0}{P_t(\beta_1)} & \overset{0}{P_t(\beta_2)} & \cdots & \overset{1}{P_t(\beta_t)} \end{bmatrix}$$

Define $p_1(x) = a_{11} + a_{12}x + \cdots + a_{1t}x^{t-1}$ What are the p_j's?

$p_j(x) = a_{j1} + a_{j2}x + \cdots + a_{jt}x^{t-1}$

Compute $M(x) = (x-\beta_1)\cdot(x-\beta_2)\cdot\cdots\cdot(x-\beta_t)$ $\leftarrow \deg = t$ ______ $O(t^2)$ ops in $k = \mathbb{Z}_p$.

and $q_j(x) = M(x)/(x-\beta_j) = \prod_{i \neq j}(x-\beta_i)$ $\leftarrow \deg = t-1$ ______ $t\,O(t) = O(t^2)$.

So $q_1(x) = (x-\beta_2)(x-\beta_3)\cdots(x-\beta_t) = 1x^{t-1} + \cdots$

Notice $q_1(\beta_1) = \prod_{i=2}^{t}(\beta_1 - \beta_i) \neq 0$. But $q_1(\beta_j) = 0$ for $j \geq 2$.

Take $p_1(x) = q_1(\beta_1)^{-1} q_1(x)$. So $p_1(\beta_1) = 1$

Let $p_j(x) = \underbrace{q_j(\beta_j)^{-1}}_{\text{Horner}} \cdot \underbrace{q_j(x)}_{t \text{ mults}}$ for $1 \leq j \leq t$. $\xleftarrow{t-1}$

______ Horner ______ $t \cdot O(t) = O(t^2)$

______ $t \cdot t \in O(t^2)$

Now $A \cdot a = b \Rightarrow a = A^{-1} b = \begin{bmatrix} - p_1 - \\ - p_2 - \\ \vdots \\ - p_t - \end{bmatrix} \begin{bmatrix} | \\ b \\ | \end{bmatrix}$.

So Let $\bar{p}_j = [\mathrm{coeff}(p_j(x), x^i) : 0 \leq i \leq t-1]$.

Then $a_j = \bar{p}_j \cdot b$ ______ $t \cdot O(t) = O(t^2)$

↑ dot product $t\times$ and $t-1$ $+$ $\quad$ $+$

$5\,O(t^2) \in O(t^2)$

We can implement this method for solving $Va = b$ using two arrays of size $t+1$ and t for $M(x)$ and $q_j(x)$. So $O(t)$ space in total.

Solving transposed Vandermonde systems of size $t \times t$.

	# arith. ops. in k.	space
Gaussian elimination	$O(t^3)$	$O(t^2)$.
Zippel 1990	↓ $O(t^2)$	↓ $O(t)$.
Kaltofen / Yagati (PhD.) 1989.	$O(M(t) \log t)$ ↑ multiply 2 polys of degree $\leq t$.	$O(t \log t)$.