Solving Transposed Vandermonde Systems

October 13, 2021 11:10 PM

Suppose $a(x,y) = \sum_{j=1}^{t} a_j M_j(x,y)$ where the monomials M_j are given.

Let $\alpha_1, \alpha_2 \in \mathbb{Z}_p$ be chosen at random.

Given $V_i = a(\alpha_1^i, \alpha_2^i)$ for $0 \le i \le t-1$ find $a_i \in \mathbb{Z}_p$.

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

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

$$\Rightarrow V_i = \sum_{j=1}^{t} a_j \beta_j^i \quad \text{for } 0 \le i \le t-1$$

A Transposed Vandermonde system.

$$\Rightarrow \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \cdots & \beta_t \\ \beta_1^2 & \beta_2^2 & \cdots & \beta_t^2 \\ \vdots & & & \\ \beta_1^{t-1} & \beta_2^{t-1} & \cdots & \beta_t^{t-1} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_t \end{bmatrix} = \begin{bmatrix} V_0 \\ V_1 \\ \vdots \\ V_{t-1} \end{bmatrix}$$

A a V

Th: $\det(A) \neq 0$ $\Leftrightarrow \beta_i \neq \beta_j$ $\Leftrightarrow M_i(\alpha_1,\alpha_2) \neq M_i(\alpha_1,\alpha_2)$ check!

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

A — $P_1(\beta_1) = 1$, $P_1(\beta_2) = 0$, $P_1(\beta_t) = 0$; $P_2(\beta_1) = 0$, $P_2(\beta_2) = 1$, $P_2(\beta_t) = 0$

Define $P_1(x) = a_{11} + a_{12}x + \cdots + a_{1t}x^{t-1}$

$P_2(x) = a_{21} + a_{22}x + \cdots + a_{2t}x^{t-1}$

$\vdots$

Let $M(x) = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_t)$ — $O(t^2)$

Let $q_j(x) = M(x)/(x-\beta_j)$ for $1 \le j \le t$ $O(t) \cdot t$

$$\Rightarrow P_j(x) = \underbrace{q_j(\beta_j)^{-1}}_{O(t)} \cdot \underbrace{q_j(x)}_{O(t)} \quad \text{for } 1 \le j \le t. \quad O(t) \cdot t$$

Now $A\underline{a} = V \Rightarrow a = A^{-1} \cdot V = \begin{bmatrix} — & P_1 & — \\ — & P_2 & — \\ & \vdots & \\ — & P_t & — \end{bmatrix} \begin{bmatrix} | \\ V \\ | \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_t \end{bmatrix}$

$\Rightarrow$ Compute $P_j = [a_{j1}\ a_{j2} \cdots a_{jt}]$

$a_j = P_j \cdot V$ for $1 \le j \le t$ $t \cdot t \in O(t^2)$.

$$P_1(x) = C_1 \prod_{i=2}^{t} (x - \beta_i) = C_1 \cdot q_1(x)$$

$$1 = P_1(\beta_1) = C_1 \cdot q_1(\beta_1) \Rightarrow C_1 = q_1(\beta_1)^{-1}$$

$P_2(x) = C_2 \cdot q_2(x)$

$C_2 = q_2(\beta_2)^{-1}$

The total cost $\approx 4\,O(t^2) = O(t^2)$ arith. ops. in $\mathbb{Z}_p$.

Oh no $V_1 = a(1,1)$ ← not random. could be an unlucky eval point.

Solution use $V_i = a(\alpha_1^i, \alpha_2^i)$ for $1 \le i \le t$.

Now

$$A = \begin{bmatrix} \beta_1 & \beta_2 & \cdots & \beta_t \\ \beta_1^2 & \beta_2^2 & & \beta_t^2 \\ \vdots & & & \\ \beta_1^t & \beta_2^t & \cdots & \beta_t^t \end{bmatrix} = \begin{bmatrix} 1 & 1 & & 1 \\ \beta_1 & \beta_2 & & \beta_t \\ \vdots & & & \\ \beta_1^{t-1} & \beta_2^{t-1} & \cdots & \beta_t^{t-1} \end{bmatrix} \begin{bmatrix} \beta_1 & & & \\ & \beta_2 & & \\ & & \ddots & \\ & & & \beta_t \end{bmatrix}.$$