Ben-Or Tiwari Sparse Interpolation

November 28, 2023 9:15 AM

Let B be a black-box for $f \in \mathbb{Z}[x_1, \dots, x_n]$.

$$\alpha \in \mathbb{Z}^n \longrightarrow \overset{B}{\boxed{\;f\;}} \longrightarrow f(\alpha).$$

Let $f = \sum_{i=1}^{t} a_i \cdot M_i(x_1, \dots, x_n)$ where $a_i \in \mathbb{Z} \setminus \{0\}$.

Let $d_i = \deg(f, x_i)$.

The interpolation problem is given B find $a_i, M_i(x_1, \dots, x_n)$.

Zippel's algorithm needs $\leq \left(\sum_{i=1}^{n} d_i t\right) + 1$. points (probes).

Ben-Or/Tiwari 1988 needs $2T$ points where $T \geq t$. ?

Try $T = 1, 2, 4, 8, 16, 32, \dots$ until it works.

It must work when $T \geq t$.

(1) Assume $T \geq t$.

Compute $v_j = f(2^j, 3^j, 5^j, \dots, p_n^j)$ for $j = 0, 1, \dots, 2T-1$. Any primes work.

Let $m_i = M_i(2, 3, 5, \dots, p_n)$ be the monomial evaluations. Are distinct.

Suppose we can determine t and m_i.

If $M_i = x_1^{d_1} \cdot x_2^{d_2} \cdots x_n^{d_n}$ then $m_i = 2^{d_1} 3^{d_2} \cdots p_n^{d_n}$. So $d_1, d_2, \dots, d_n$ can be determined by $\div$ m_i by $2, 3, 5, \dots, p_n$ repeatedly.

E.g. if $n=3$, $m_i = 300 = 3 \cdot 10^2 = 2^2 \cdot 3 \cdot 5^2 \Rightarrow M_i = x_1^2 x_2 x_3^2$.

How do we determine the coefficients a_i's ?

Observe
$$\begin{aligned} M_i(2^j, 3^j, \dots, p_n^j) &= (2^j)^{d_1} \cdot (3^j)^{d_2} \cdots (p_n^j)^{d_n} \\ &= (2^{d_1})^j (3^{d_2})^j \cdots (p_n^{d_n})^j \\ &= M_i(2, 3, \dots, p_n)^j \\ &= m_i^j. \end{aligned}$$

So $f(2^j, 3^j, \dots, p_n^j) = \sum_{i=1}^{t} a_i M_i(2^j, 3^j, \dots, p_n^j) = m_i^j$.

Consider

$$V = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ m_1 & m_2 & \cdots & m_t \\ m_1^2 & m_2^2 & \cdots & m_t^2 \\ \vdots & & & \\ m_1^{t-1} & m_2^{t-1} & \cdots & m_t^{t-1} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_t \end{bmatrix} = \begin{bmatrix} f(1,1,\dots,1) = v_1 \\ f(2,3,\dots,p_n) = v_2 \\ \vdots \\ v_t \end{bmatrix}$$

V^T is a Vandermonde system. We can solve $Va = v$ in $O(t^2)$ arith. ops. in $\mathbb{Q}$ using Zippel's 1990 solver.

② How to determine m_i's ?

Let $\lambda(z) = \prod_{i=1}^{t} (z - m_i) = \lambda_0 + \lambda_1 \cdot z + \dots + \lambda_{t-1} z^{t-1} + z^t$.

We will solve a linear system to get the λ_i's then compute the roots of $\lambda(z)$ in $\mathbb{Z}$ by factoring $\lambda(z)$.

```
> roots(f);          # computes the roots in Q
> Roots(f) mod p;    # computes roots in Zp where p is a prime.
```

Consider

$$\sum_{i=1}^{t} a_i m_i^{\ell} \cdot \underbrace{\lambda(m_i)}_{=0} = 0 = \sum_{i=1}^{t} a_i m_i^{\ell} \left(\sum_{j=1}^{t} \lambda_j m_i^j \right) \quad \text{for } \ell = 0, 1, \dots$$

$$= \sum_{i=1}^{t} \sum_{j=1}^{t} a_i m_i^{\ell+j} \lambda_j = \sum_{j=1}^{t} \lambda_j \left(\sum_{i=1}^{t} a_i m_i^{\ell+j} \right).$$

$$\Rightarrow \lambda_0 \overbrace{\underbrace{\sum_{i=1}^{t} a_i m_i^{\ell}}_{= v_\ell}}^{j=0} + \lambda_1 \overbrace{\underbrace{\sum_{i=1}^{t} a_i m_i^{\ell+1}}_{v_{\ell+1}}}^{j=1} + \dots + \underbrace{\lambda_t}_{=1} \overbrace{\underbrace{\sum_{i=1}^{t} a_i m_i^{\ell+t}}_{v_{\ell+t}}}^{j=t} = 0 \quad \text{for } \ell = 0, 1, \dots$$

$$\Rightarrow \lambda_0 v_\ell + \lambda_1 v_{\ell+1} + \cdots + \lambda_{t-1} v_{\ell+t-1} = -v_{\ell+t}.$$

$$\begin{array}{c} \ell=0 \\ \ell=1 \\ \\ \\ \ell=t-1 \end{array} \underbrace{\begin{bmatrix} v_0 & v_1 & \cdots & v_{t-1} \\ v_1 & v_2 & \cdots & v_t \\ \vdots & & & \\ v_{t-1} & v_t & \cdots & v_{2t-2} \end{bmatrix}}_{H_t} \underbrace{\begin{bmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_{t-1} \end{bmatrix}}_{\lambda} = \underbrace{\begin{bmatrix} -v_t \\ -v_{t+1} \\ \vdots \\ -v_{2t-1} \end{bmatrix}}_{v}$$

H_t is a $t \times t$ Hankel Matrix.

Theorem: If $T \geq t$ then $\mathrm{rank}(H_T) = t$.

Solving $H_t \lambda = v$ can be done in $O(t^2)$ arith. ops. using either the Berlekamp–Massey algorithm or the Euclidean algorithm.

Let $d = \deg(f)$. $= x_n^d$

$m_i = M_i(2^j, 3^j, \ldots, p_n^j)$ for $j = 0, 1, \ldots, 2T-1$. 1000

m_i may be as large as $(p_n^T)^d = p_n^{d \cdot T}$.

So $\log_{10} p_n^{dT} = dT \log p_n$ digits. Very big.

Solution: the $m_i = M_i(2, 3, \ldots, p_n) \leq p_n^d$ where $d = \deg(f)$.

So pick a prime $p > m_i$.

Compute $v_j = f(2^j, 3^j, \ldots, p_n^j) \bmod p$.

Solve $H_T \cdot a = v \bmod p$ to get $\lambda(z) \bmod p$.

Compute the roots of $\lambda(z) \bmod p$.