SFU SIMON FRASER UNIVERSITY

The Fast Transposed Vandermonde Solver

Hyukho Kwon

Department of Mathematics
Simon Fraser University

April 17, 2024

Transposed Vandermonde System of Equations

Let F be a field. Let $a = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in F[x]$ where all a_is are unknown. Given $u_1, u_2, \ldots, u_n \in F$, let $b_i = a(u_i)$ for $1 \leq i \leq n$.

Let $u_i = \alpha^{i-1}$ for some $\alpha \in F$ where $\alpha^i \neq \alpha^j$ for all $i \neq j$. Then $a(u_i) = a(\alpha^{i-1}) = b_i$.

Problem: Interpolate a with $u_1, u_2, \ldots, u_n$ and $b_1, b_2, \ldots, b_n$.

$$\underbrace{\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ u_1 & u_2 & u_3 & \cdots & u_n \\ u_1^2 & u_2^2 & u_3^2 & \cdots & u_n^2 \\ \vdots & \vdots & \vdots & & \vdots \\ u_1^{n-1} & u_2^{n-1} & u_3^{n-1} & \cdots & u_n^{n-1} \end{bmatrix}}_{U} \underbrace{\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{bmatrix}}_{\mathbf{a}} = \underbrace{\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_n \end{bmatrix}}_{\mathbf{b}}$$

We call $U\mathbf{a} = \mathbf{b}$ a transposed Vandermonde system of equations.

Methods	# ops in F	space
Gaussian Elimination	$O(n^3)$	$O(n^2)$
Zippel's method [3]	$O(n^2)$	$O(n)$
Kaltofen & Yagati's method [2]	$O(M(n)\log n)$	$O(n\log n)$

$M(n)$ is the number of arithmetic operations in F for polynomial multiplication where the sum of the degrees of two polynomials is less than $2n$.

n	Zippel TVS	ratio	BUPT	DDPT1	DDPT2	FastTVS	ratio	speed up
2^6	0.1270	-	0.02	0.042	0.041	0.132	-	0.96
2^7	0.4830	3.80	0.047	0.109	0.096	0.309	2.34	1.56
2^8	1.9249	3.99	0.128	0.243	0.236	0.875	2.83	2.19
2^9	7.5300	3.91	0.303	0.654	0.653	2.055	2.35	3.66
2^{10}	30.091	4.00	0.768	1.965	1.979	5.664	2.76	5.31
2^{11}	119.46	3.97	1.929	6.313	6.397	16.677	2.94	7.16
2^{12}	476.21	3.99	4.556	17.676	17.719	44.234	2.65	10.76
2^{13}	1,903.1	4.00	10.692	46.762	46.306	112.81	2.55	16.86
2^{14}	7,617.6	4.00	24.734	116.68	116.82	277.05	2.46	27.49
2^{15}	30,629	4.02	58.236	284.83	285.75	670.03	2.42	45.71
2^{16}	122,162	3.99	130.42	678.51	681.43	1,575.4	2.35	77.54

Table: CPU timings in *ms* for solving $n \times n$ transposed Vandermonde system over $\mathbb{Z}_p$ with $p = 3 \cdot 2^{30} + 1$

Product Tree

Kaltofen and Yagati's method utilized Borodin and Munro's product tree [1] for polynomial multipoint evaluation algorithm with distinct evaluation points $u_1, u_2, \ldots, u_n \in F$ where $n = 2^k$ for some $k \in \mathbb{N}$.